Security as Development

Ryan Huber
Slack

@ryanhuber

A keynote in three acts

Preface: The Origin Story

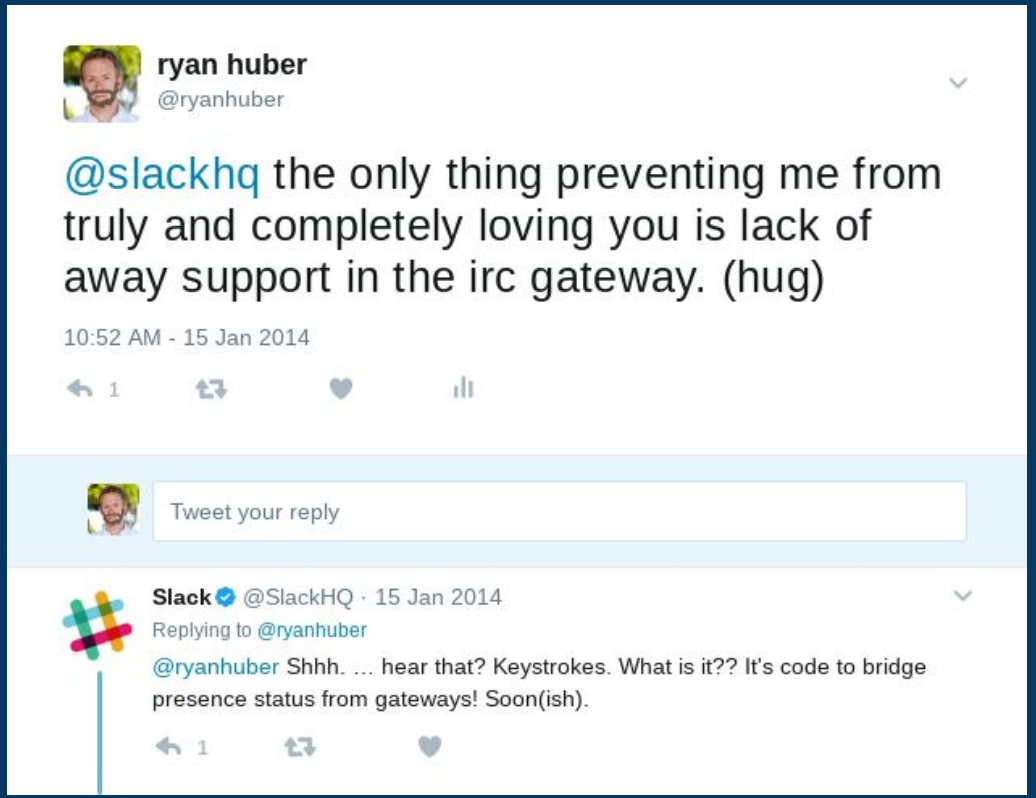
Slack (beta)

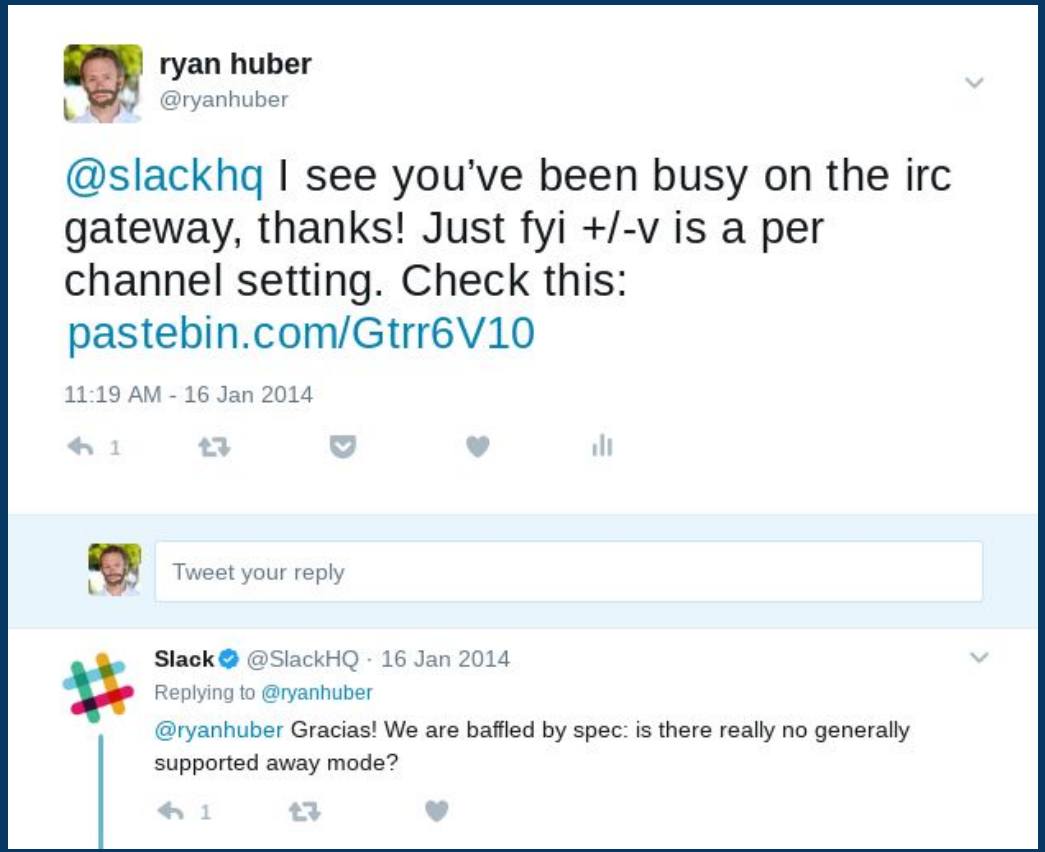
:rage_emoji:

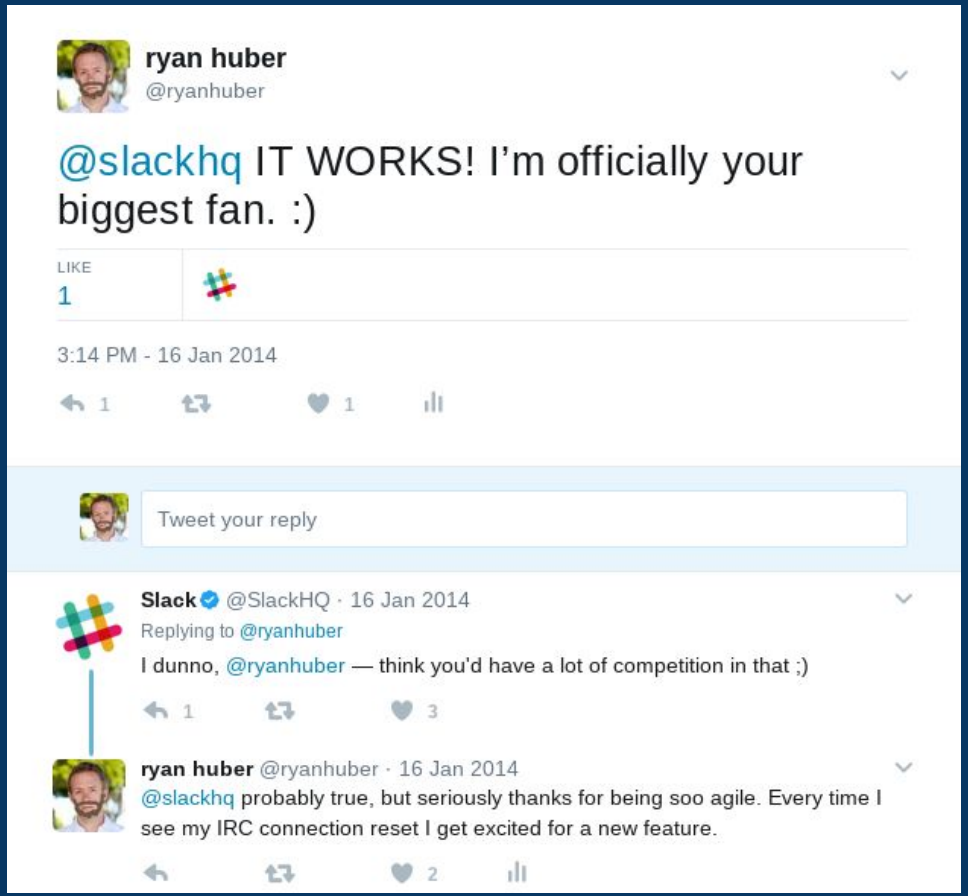
The command line is my ~

I use WeeChat

IRC Gateway


ryan huber
@ryanhuber
@slackhq the only thing preventing me from truly and completely loving you is lack of away support in the irc gateway. (hug)
10:52 AM - 15 Jan 2014
1
Tweet your reply
Slack @SlackHQ · 15 Jan 2014
Replying to @ryanhuber
@ryanhuber Shhh. ... hear that? Keystrokes. What is it?? It's code to bridge presence status from gateways! Soon(ish).
1


ryan huber
@ryanhuber
@slackhq I see you've been busy on the irc gateway, thanks! Just fyi +/-v is a per channel setting. Check this: pastebin.com/Gtrr6V10
11:19 AM - 16 Jan 2014
1
Tweet your reply
Slack @SlackHQ · 16 Jan 2014
Replying to @ryanhuber
@ryanhuber Gracias! We are baffled by spec: is there really no generally supported away mode?
1


ryan huber
@ryanhuber
@slackhq IT WORKS! I'm officially your biggest fan. :)
LIKE
1
3:14 PM - 16 Jan 2014
1
1
Tweet your reply
Slack @SlackHQ · 16 Jan 2014
Replying to @ryanhuber
I dunno, @ryanhuber — think you'd have a lot of competition in that ;)
1
3
ryan huber @ryanhuber · 16 Jan 2014
@slackhq probably true, but seriously thanks for being soo agile. Every time I see my IRC connection reset I get excited for a new feature.
2

Features

wee-slack

wee-slack / **wee-slack**

Watch 40 | Star 618 | Fork 88

Code | Issues 54 | Pull requests 10 | Projects 0 | Pulse | Graphs

A WeeChat plugin for Slack.com. Synchronizes read markers, provides typing notification, search, etc..

882 commits | **7** branches | **2** releases | **38** contributors | MIT

Birthday party

MAT HONAN GEAR 08.07.14 6:30 AM

THE MOST FASCINATING PROFILE YOU'LL EVER READ ABOUT A GUY AND HIS BORING STARTUP

So I asked if I could work there...

… and I was hired!

🎉🎉🎉🎉🎉

```
61    elif args.startswith("nickup2"):
62      text = args.split()[1:]
63      for s in text:
64        browser.open("https://%s/account/settings" % (domain))
65        browser.select_form(nr=0)
66        name = s
67        browser.form['username'] = "a---" + name
68        reply = browser.submit()
69      browser.open("https://%s/account/settings" % (domain))
70      browser.select_form(nr=0)
71      browser.form['username'] = nick
72      reply = browser.submit()
```

Note that you cannot change your username more than twice per hour. Choose wisely.

Looking back

The first message I found..

myles 3:33 PM

it's this fucking guy again:

Act 1:
Get To Work

The good

Veteran web developers

DevOps/CI

Bug bounty

I started exploring

Confession:
I also spent a LOT of time updating my client.

Networking
(the human kind)

Basic risk

Credential theft is how most breaches start

2fa

Backend auth

Duo Security

Ann Arbor, MI http://www.duosecurity.com

ssh

EC2 Classic

Bastions

54:1

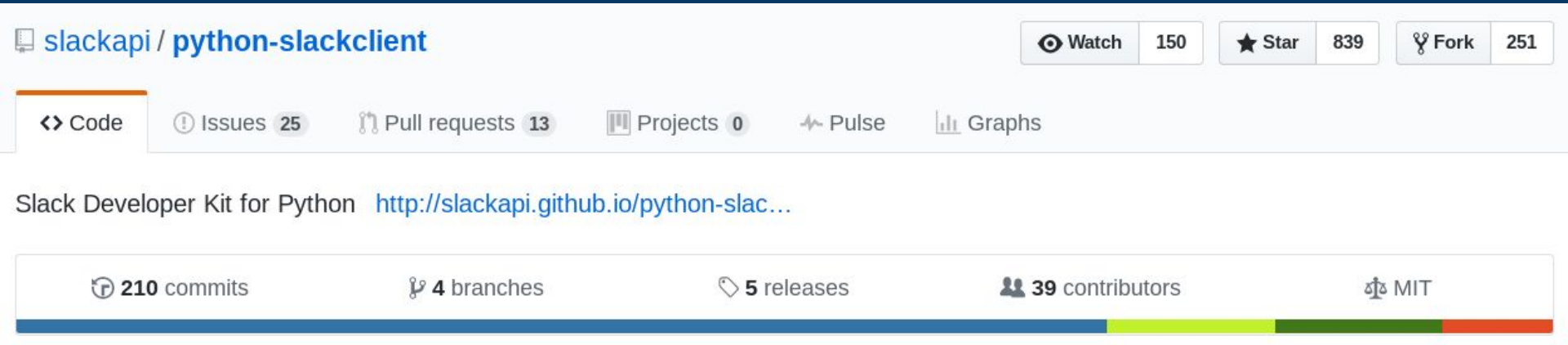
But this is Slack..

Bots

“Use tools in preference to unskilled help to lighten a programming task, even if you have to detour to build the tools and expect to throw some of them out after you've finished using them.”

- Doug McIlroy, Bell System Technical Journal, 1978

python-slackclient



python-rtmbot

slackhq / **python-rtmbot**

Watch 150 | Star 477 | Fork 252

Code | Issues 11 | Pull requests 9 | Projects 0 | Pulse | Graphs

No description, website, or topics provided.

141 commits | **1** branch | **4** releases | **17** contributors | MIT

BountyBot

YubiKeys

This is fine

Act 2:
Unexpected Challenges

Our first red team exercise

Slack Follow

Making your working life simpler, more pleasant, and more productive

Mar 27, 2015 · 4 min read

March 2015 security incident and the launch of Two Factor Authentication

We were recently able to confirm that there was unauthorized access to a Slack database storing user profile information. We have since blocked this unauthorized access and made additional changes to our technical infrastructure to prevent future incidents. We have also released two factor authentication and we strongly encourage all users to enable this security feature.

We need this room

I need the credit card

dd

Disk timelines

Silos of data

Lots of `grep -F`

Review every commit + config management

A reason to love :cloud:

3 days

Notification

We were lucky

Being lucky is great, but..

Act 3: Being good

Hiring

SecOps

Building

SecOps VPC

Vault

hashicorp / **vault**

Watch 278 | Star 6,595 | Fork 849

Code | Issues 200 | Pull requests 34 | Projects 0 | Pulse | Graphs

A tool for managing secrets. https://www.vaultproject.io/

5,563 commits | **33** branches | **35** releases | **292** contributors | MPL-2.0

Elasticsearch

go-audit

slackhq / **go-audit**

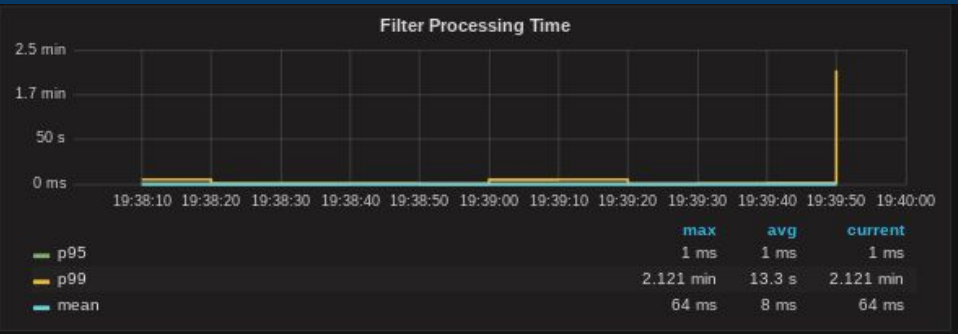
Watch 37 | Star 732 | Fork 32

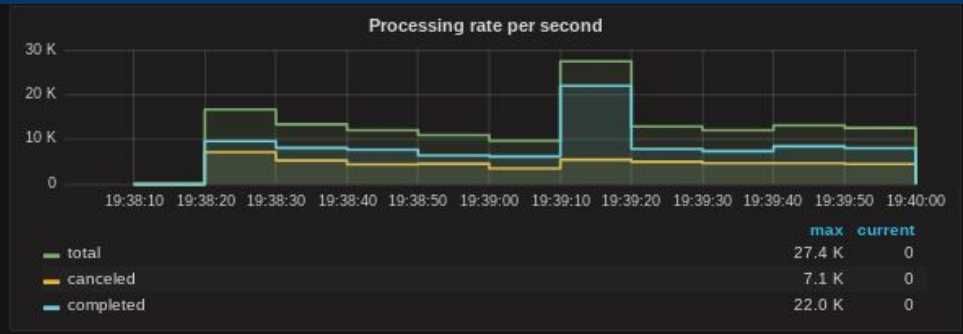
Code | Issues 1 | Pull requests 2 | Projects 0 | Pulse | Graphs

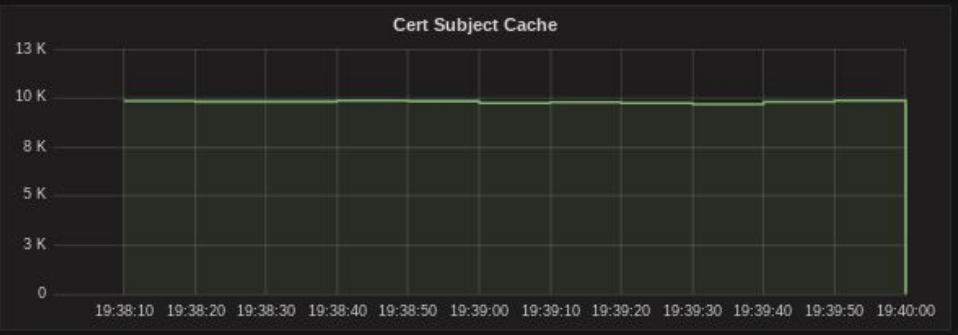
go-audit is an alternative to the auditd daemon that ships with many distros

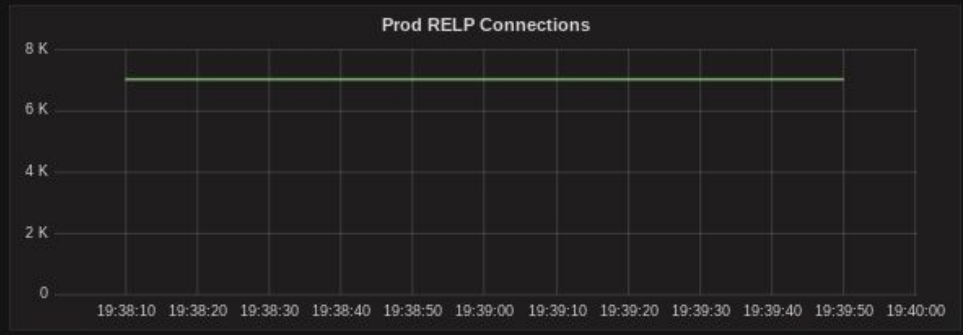
134 commits | **3** branches | **0** releases | **4** contributors | MIT

Every important syscall from every server

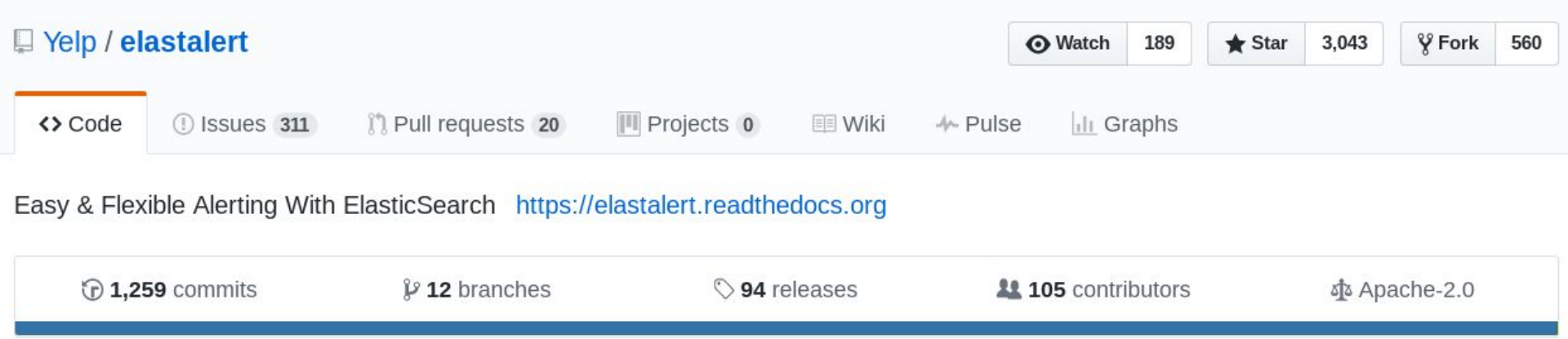

Filter Processing Time
2.5 min
1.7 min
50 s
0 ms
19:38:10 19:38:20 19:38:30 19:38:40 19:38:50 19:39:00 19:39:10 19:39:20 19:39:30 19:39:40 19:39:50 19:40:00
max avg current
p95 1 ms 1 ms 1 ms
p99 2.121 min 13.3 s 2.121 min
mean 64 ms 8 ms 64 ms


Processing rate per second
30 K
20 K
10 K
0
19:38:10 19:38:20 19:38:30 19:38:40 19:38:50 19:39:00 19:39:10 19:39:20 19:39:30 19:39:40 19:39:50 19:40:00
max current
total 27.4 K 0
canceled 7.1 K 0
completed 22.0 K 0


Cert Subject Cache
13 K
10 K
8 K
5 K
3 K
0
19:38:10 19:38:20 19:38:30 19:38:40 19:38:50 19:39:00 19:39:10 19:39:20 19:39:30 19:39:40 19:39:50 19:40:00


Prod RELP Connections
8 K
6 K
4 K
2 K
0
19:38:10 19:38:20 19:38:30 19:38:40 19:38:50 19:39:00 19:39:10 19:39:20 19:39:30 19:39:40 19:39:50 19:40:00

ElastAlert


Yelp / elastalert
Watch 189
Star 3,043
Fork 560
Code
Issues 311
Pull requests 20
Projects 0
Wiki
Pulse
Graphs
Easy & Flexible Alerting With ElasticSearch https://elastalert.readthedocs.org
1,259 commits
12 branches
94 releases
105 contributors
Apache-2.0

AlertCenter

Deputizing everyone

Securitybot

Do your best to avoid annoying people

Upstream contributions

So we’re done, right?

Epilogue

Red Team

On a Sunday

A low severity alert

IR Begins

We did ok once

Continuous improvement + building

The security team is now 14 people

Incident Response
ProdSec
Risk & Compliance
SecOps

Summary

How to hire your first security person

You can’t buy security

Invest in people

The breach taught us a lot

Be nice

Obrigado!