Resilient Software Engineering

Swiss Cyber Storm - Lucerne Switzerland - 2016-10-19

Nick Galbreath nickg@signalsciences.com

Signal Sciences

It’s Online!

https://speakerdeck.com/ngalbreath
resilient-software-engineering

I’m Online!

@ngalbreath

Context And Disclosure

- Software engineering background
- Web application background
- I’m a vendor, but this is not a vendor talk.

100-10-1
Dev-Ops-Sec

👨 👨 👨 👨 👨 👨 👨 👨 👨 👨

👨 👨 👨 👨 👨 👨 👨 👨 👨 👨

👨 👨 👨 👨 👨 👨 👨 👨 👨 👨

👨 👨 👨 👨 👨 👨 👨 👨 👨 👨 👨 👨 👨 👨 👨

👨 👨 👨 👨 👨 👨 👨 👨 👨 👨 👨 👨 👨 👨 👨 😱

SF Bay Area

For every 1 person in infosec, there are 2 job postings

100-10-3
Dev-Ops-Sec

👨👨👨👨👨👨👨👨👨👨

👨👨👨👨👨👨👨👨👨👨

👨👨👨👨👨👨👨👨👨👨

👨👨👨👨👨👨👨👨👨👨👨👨👨👨👨😱

👨👨👨👨👨👨👨👨👨👨👨👨👨👨👨😱😱

Can We Turn Security Problems into Engineering Problems?

100x Increase in Resources

- Not Your Code
- Your Code
- Getting Your Code To Production
- Monitoring Your Code
- When Your Code Fails

Not Your Code

Your Application is 75%
Open Source Software

Fact Check

```
$ find vendor -name '*.go' | xargs cat | wc -l
116324
$ find . -name '*.go' | xargs cat | wc -l
149496
$ dc 116324.0 149496.0 div 100 mul p
77.8108
```

```
$ find vendor -name '*.go' | xargs cat | wc -l
505970
$ find . -name '*.go' | xargs cat | wc -l
646517
$ dc 505970 646517 div 100 mul p
78.2609
```

Oh did I Include Linked C Libraries?

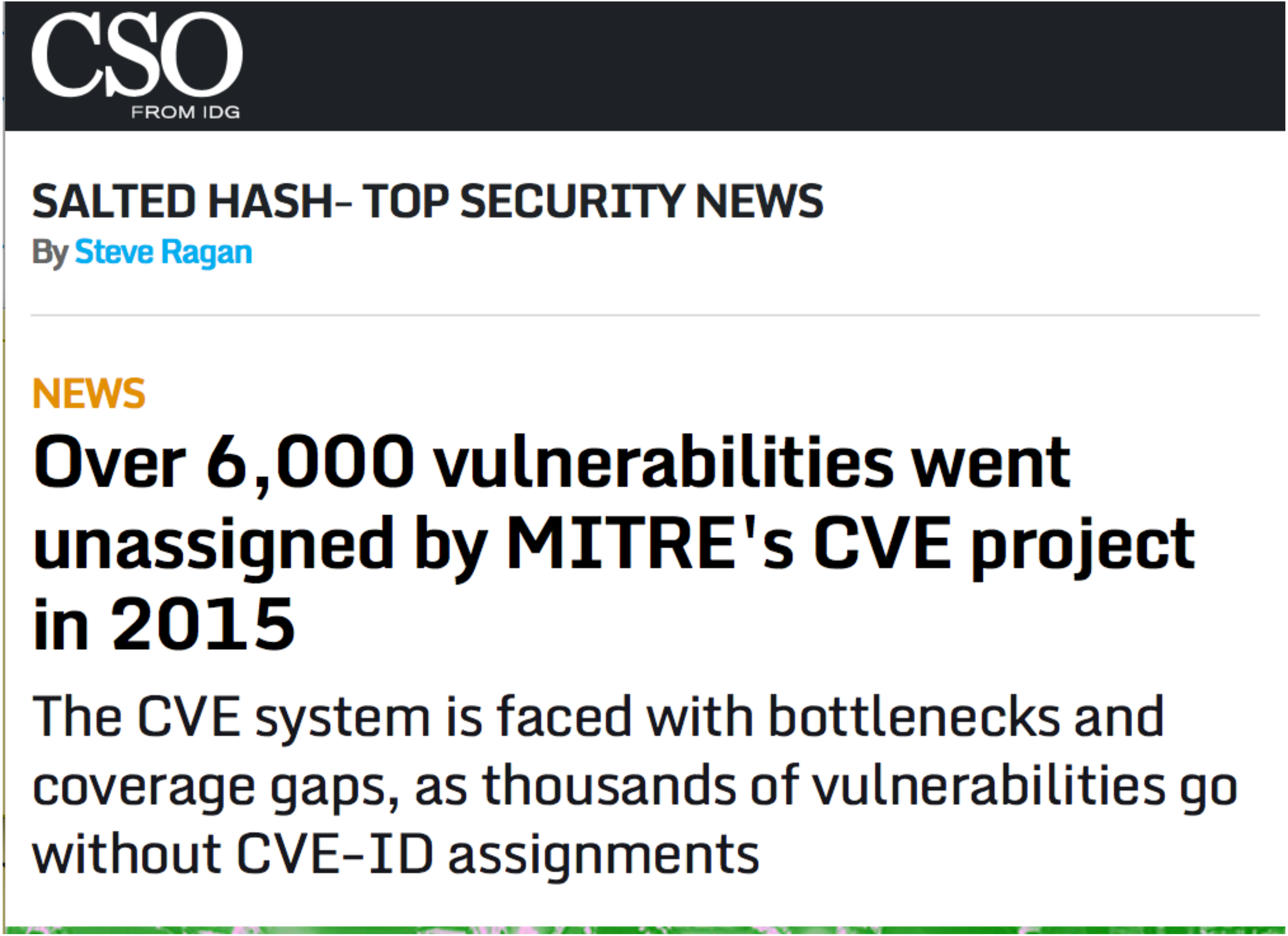
Which
ruby/python/node/php
modules
require C libraries?

Where did this come from?

- The OS ?
- The Ops Team building an image ?
- The Dev Team building a container or just vendoring / copying code?

Is It Up To Date?

- If you are not using OS provided packages, how do you know?
- If you are using the OS provided packages, staying to date is great, but..



CSO
FROM IDG

SALTED HASH- TOP SECURITY NEWS

By Steve Ragan

NEWS

Over 6,000 vulnerabilities went unassigned by MITRE's CVE project in 2015

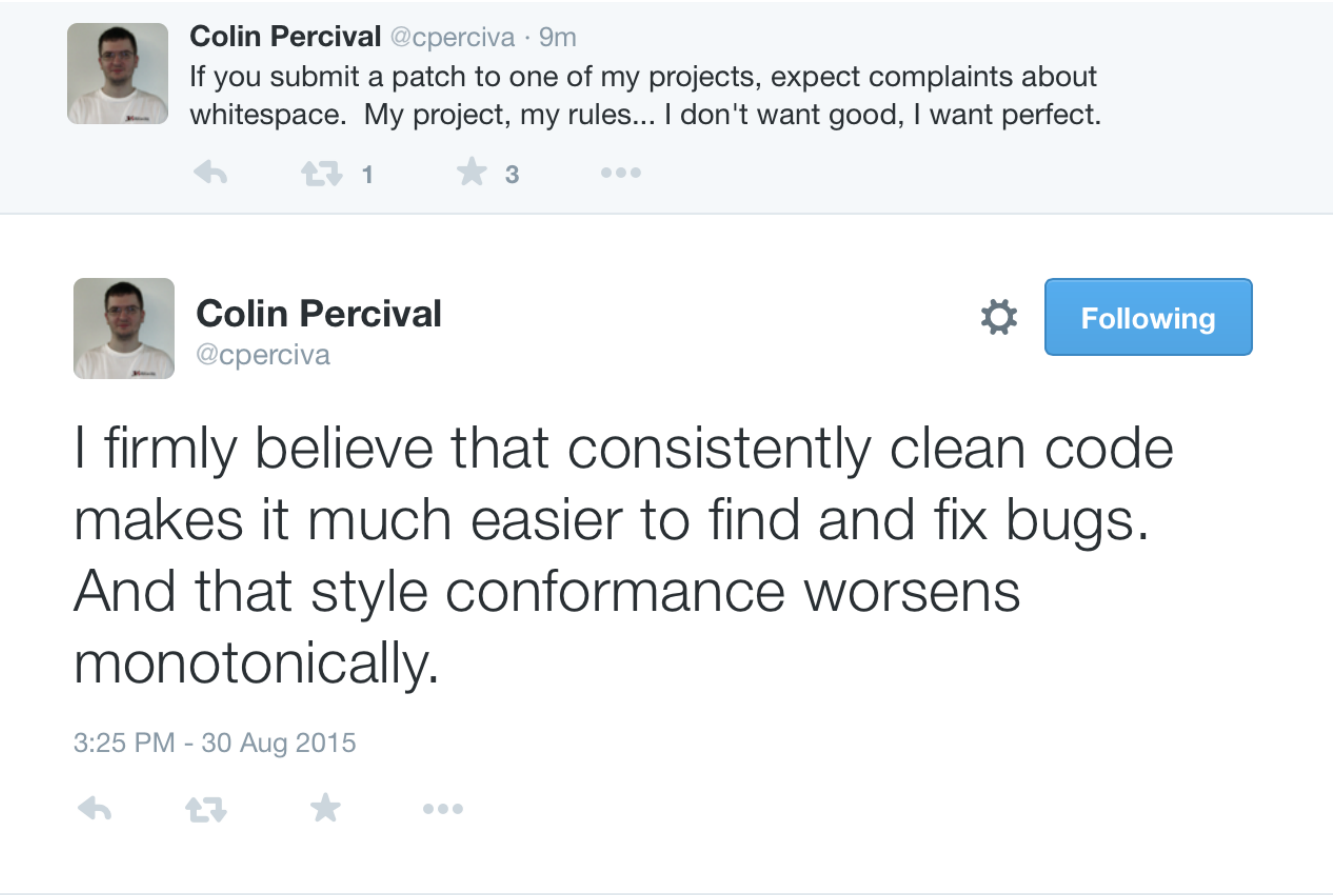
The CVE system is faced with bottlenecks and coverage gaps, as thousands of vulnerabilities go without CVE-ID assignments

2016-10-22 http://www.csoonline.com/article/3122460/techology-business/over-6000-vulnerabilities-went-unassigned-by-mitres-cve-project-in-2015.amp.html

How is 3rd Party Software Managed?

The Software Supply Chain is a Security Issue

Your Code



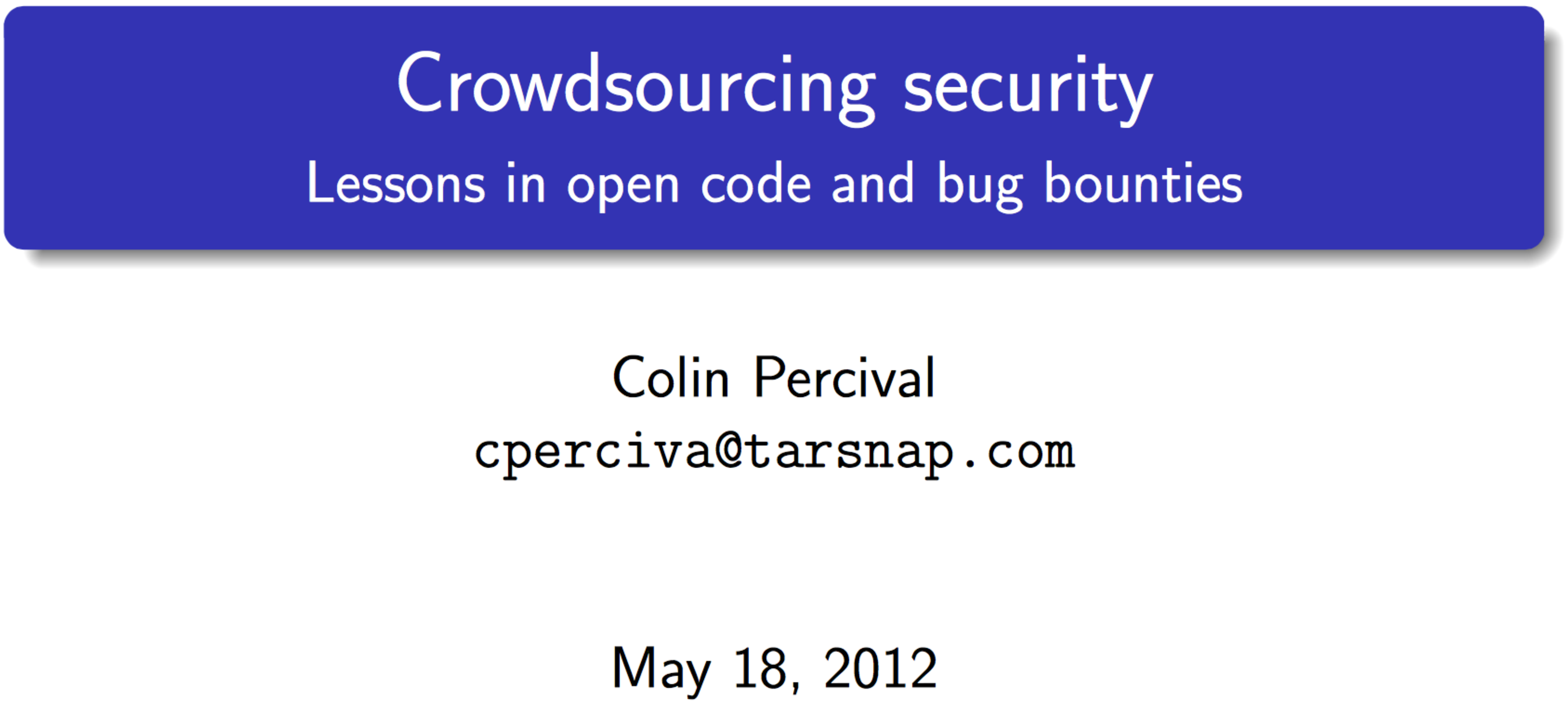
Colin Percival @cperciva · 9m

If you submit a patch to one of my projects, expect complaints about whitespace. My project, my rules... I don't want good, I want perfect.

Colin Percival
@cperciva

I firmly believe that consistently clean code makes it much easier to find and fix bugs. And that style conformance worsens monotonically.

3:25 PM - 30 Aug 2015



Crowdsourcing security

Lessons in open code and bug bounties

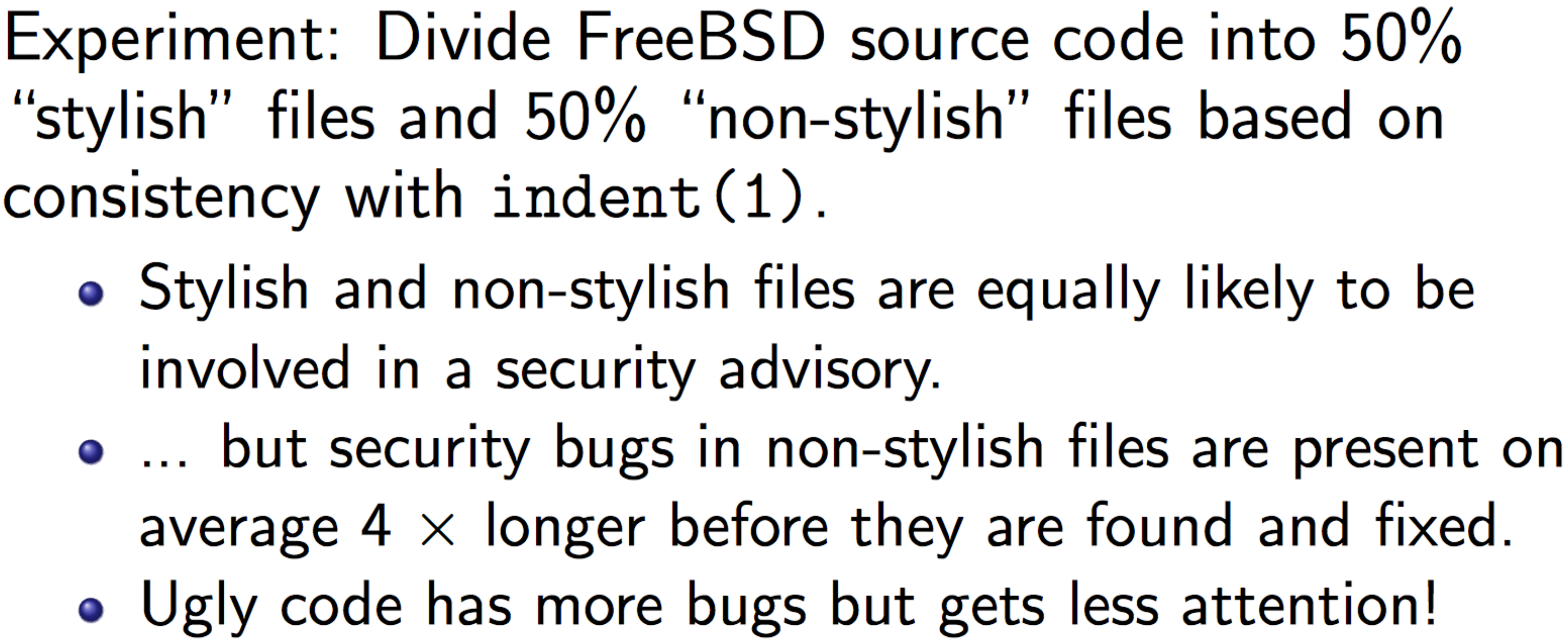
Colin Percival

cperciva@tarsnap.com

May 18, 2012

https://www.bsdcan.org/2012/schedule/attachments/218_crowdsec.pdf

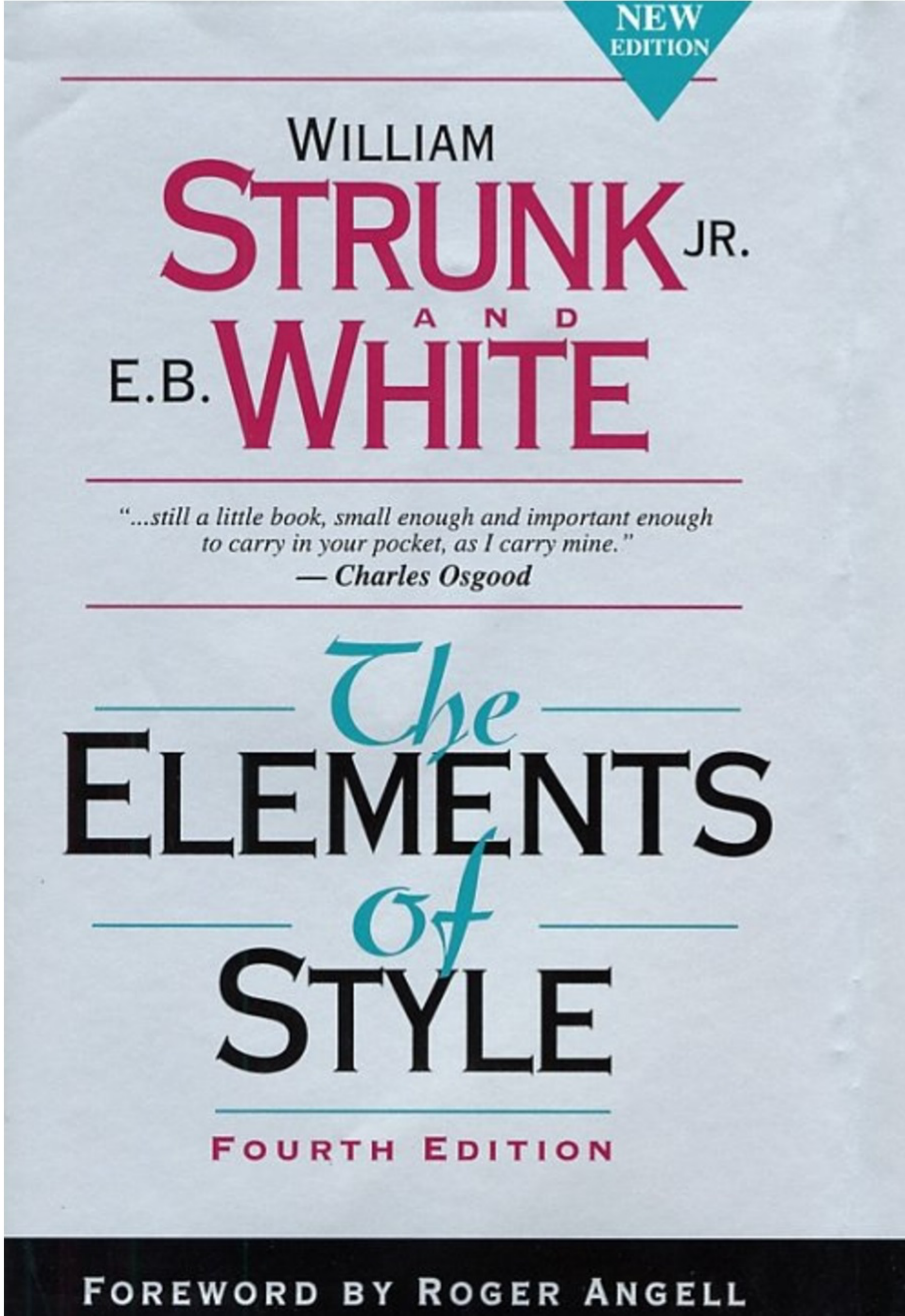
The Buried Lead:
4x Faster Bug Fixes



Experiment: Divide FreeBSD source code into 50% “stylish” files and 50% “non-stylish” files based on consistency with `indent(1)`.

- Stylish and non-stylish files are equally likely to be involved in a security advisory.
- ... but security bugs in non-stylish files are present on average 4 × longer before they are found and fixed.
- Ugly code has more bugs but gets less attention!

Oddly relevant to software



Sound Familiar?

- 16. **Be clear**…. Even to a writer who is being intentionally obscure or wild of tongue we can say, "**Be obscure clearly!** Be wild of tongue in a way we can understand!"

- 19. **Do not take shortcuts at the cost of clarity**. Many shortcuts are self-defeating; they waste the reader's time instead of conserving it.

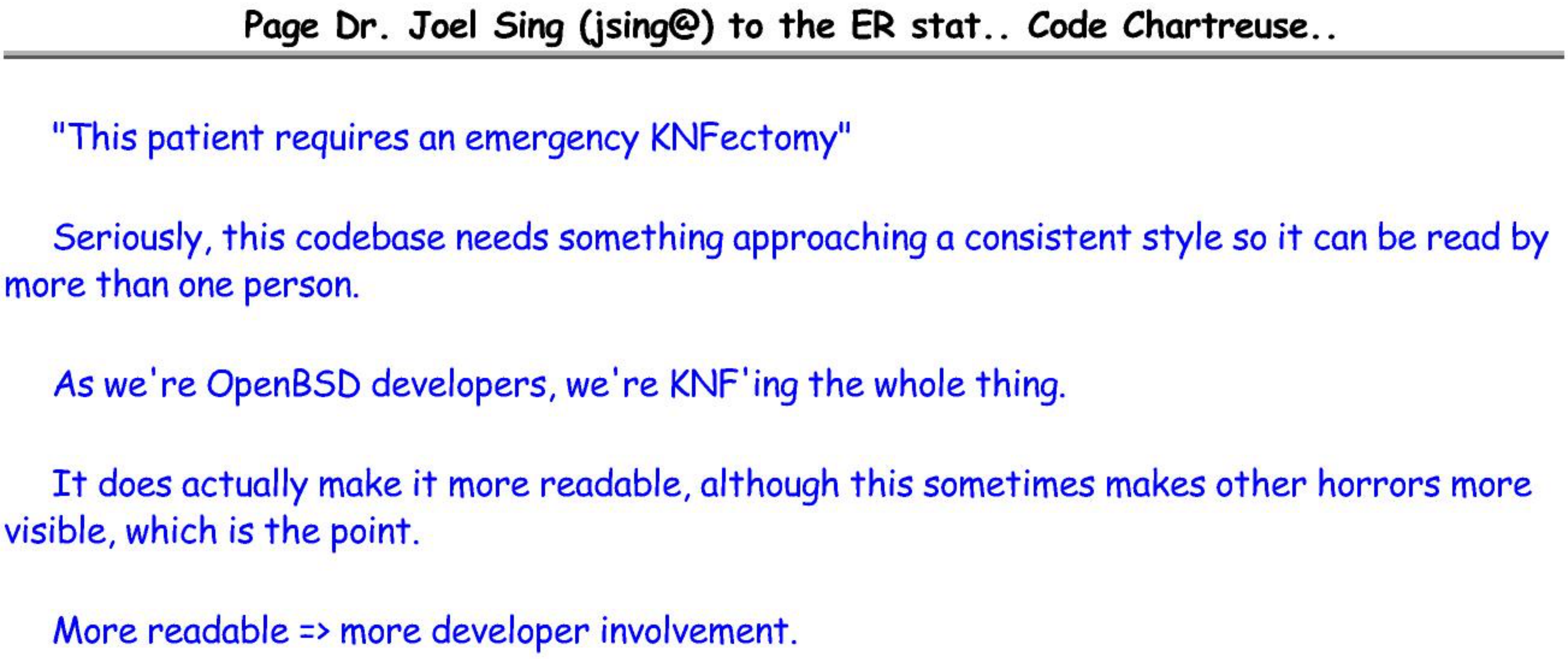
- 20. **Avoid foreign languages**. (write in the standard language, reuse existing dependencies)

- 21. **Prefer the standard to the offbeat. Young writers will be drawn at every turn toward eccentricities in language.**

OpenSSL Heartbleed

Absolutely convinced this was due to
the un-friendly un-styled code base

LibreSSL - The First 30 Days



Page Dr. Joel Sing (jsing@) to the ER stat.. Code Chartreuse..

"This patient requires an emergency KNFectomy"

Seriously, this codebase needs something approaching a consistent style so it can be read by more than one person.

As we're OpenBSD developers, we're KNF'ing the whole thing.

It does actually make it more readable, although this sometimes makes other horrors more visible, which is the point.

More readable => more developer involvement.

KNF - Kernel Normal Form C-style

http://www.openbsd.org/papers/bsdcan14-libressl/
May 18, 2014

BoringSSL

First thing mentioned? Style cleanup

So BoringSSL headers and sources look like this rather than this. The comments in BoringSSL headers can be extracted by a tool to produce documentation of a sort. (Although it could do with a make-over.)

(Clang's formatting tool and its Vim integration are very helpful! It's been the biggest improvement in my code-editing experience in many years.)

https://www.imperialviolet.org/2015/10/17/boringssl.html

Attackers Know This Too

How I Hacked Facebook, and Found Someone's Backdoor Script

Orange Tsai   http://blog.orange.tw

… **But from the fragments of source code mentioned in the Advisory, I felt that with such coding style there should still be security issues remained** in FTA if I kept looking. Therefore, I began to look for 0-Day vulnerabilities on FTA products! …. *finds 7 CVEs*

`http://devco.re/blog/2016/04/21/how-I-hacked-facebook-and-found-someones-backdoor-script-eng-ver/`

The Canonical Example, With C and PHP

```
if (something)
  do_critical();
```

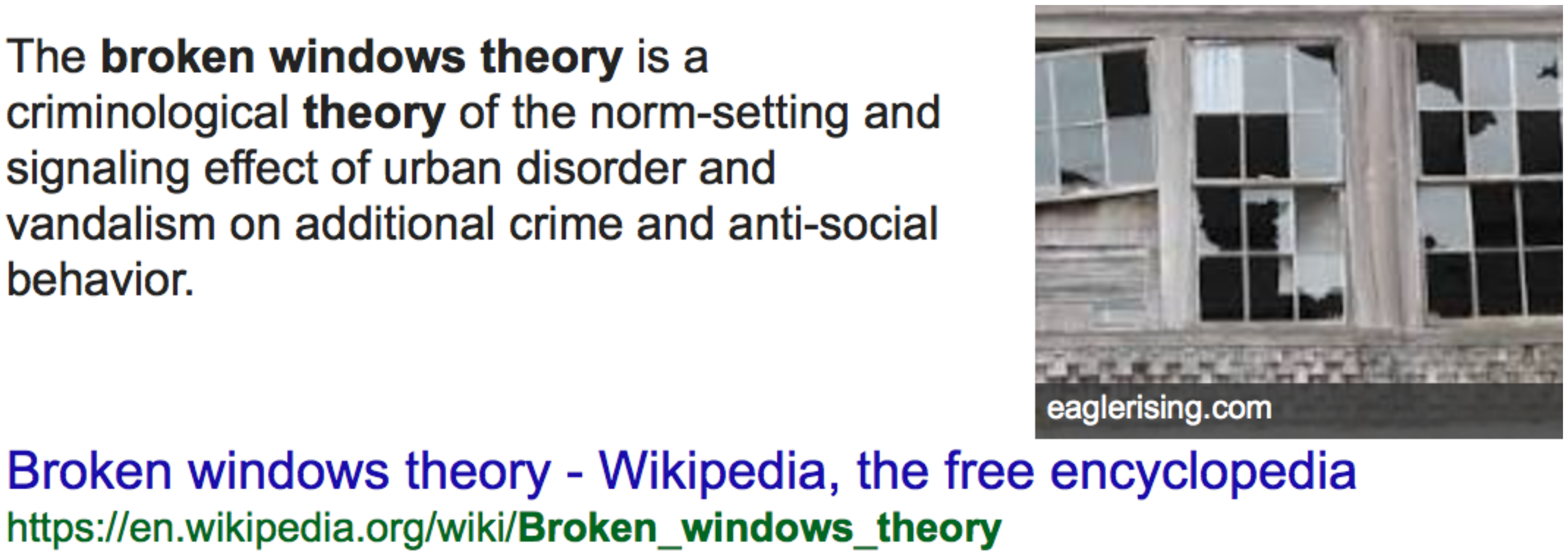
```
> log_debug(…);
```

```
if (something)
 log_debug(…);
 do_critical();
```

```
if (something)
  log_debug(…);
do_critical();
```

```
if (something) do_critical();
```

```
<-if (something) do_critical();
>+if (something) {
>+  log_debug("…");
>+  do_critical();
>+}
```



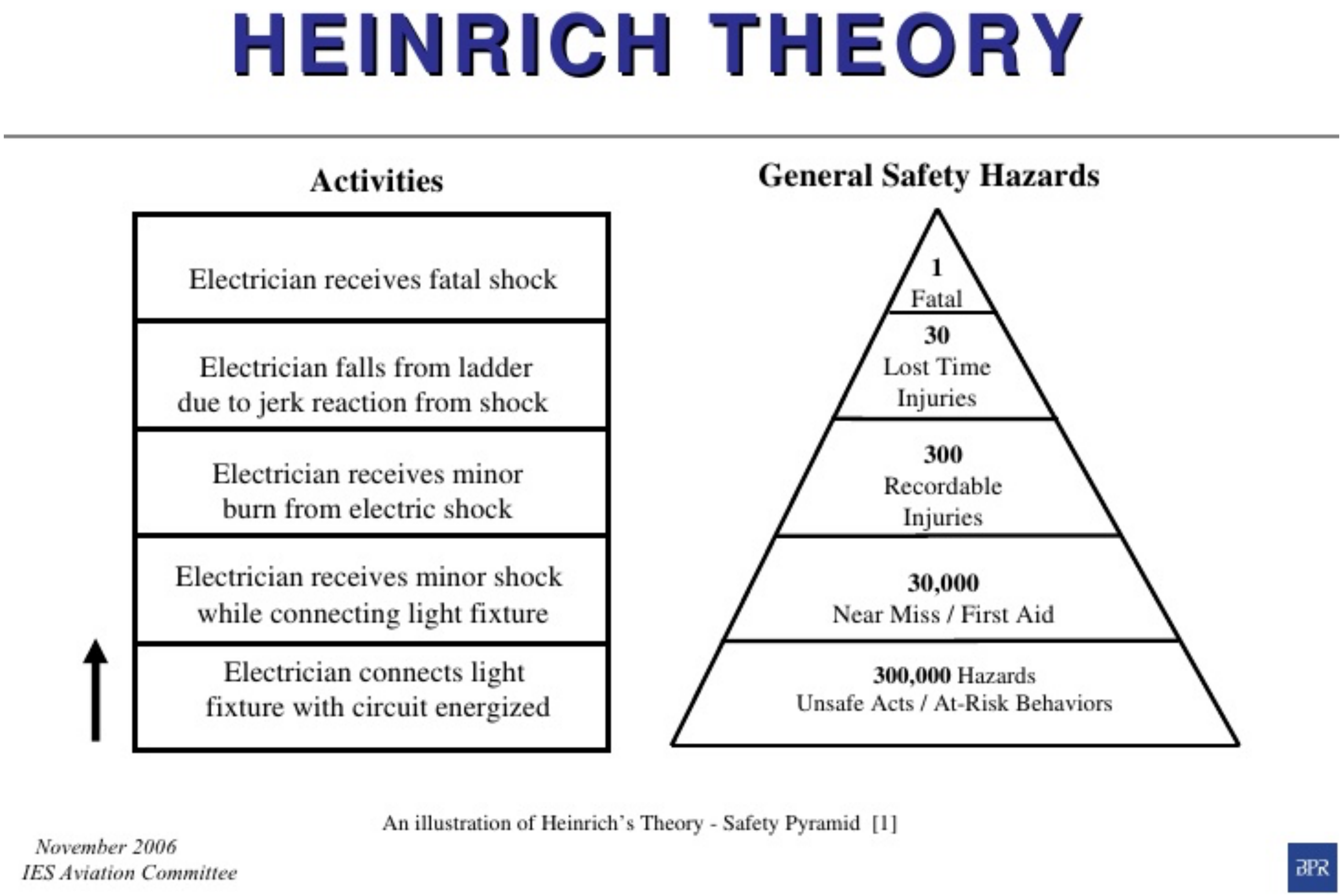
The **broken windows theory** is a criminological **theory** of the norm-setting and signaling effect of urban disorder and vandalism on additional crime and anti-social behavior.

eaglerising.com

Broken windows theory - Wikipedia, the free encyclopedia

https://en.wikipedia.org/wiki/**Broken_windows_theory**

- Lots of asterisks here. Low Data Quality,
- Cause != Correlation
- Type of Crime or Severity not well measured.
- Read on!: http://cebcp.org/.../broken-windows-policing/



HEINRICH THEORY

Activities

Electrician receives fatal shock

Electrician falls from ladder due to jerk reaction from shock

Electrician receives minor burn from electric shock

Electrician receives minor shock while connecting light fixture

Electrician connects light fixture with circuit energized

General Safety Hazards

1 Fatal

30 Lost Time Injuries

300 Recordable Injuries

30,000 Near Miss / First Aid

300,000 Hazards Unsafe Acts / At-Risk Behaviors

An illustration of Heinrich's Theory - Safety Pyramid [1]

November 2006
IES Aviation Committee

Only applies to accidents that scale linearly in severity … major failures have much more complex causes

Results

- Faster code reviews
- More code reviews
- Smaller diffs
- Less merge conflicts
- Faster bug detection
- Faster on boarding
- Side effect: simpler code.
- Easier to read for everyone, including security reviews.

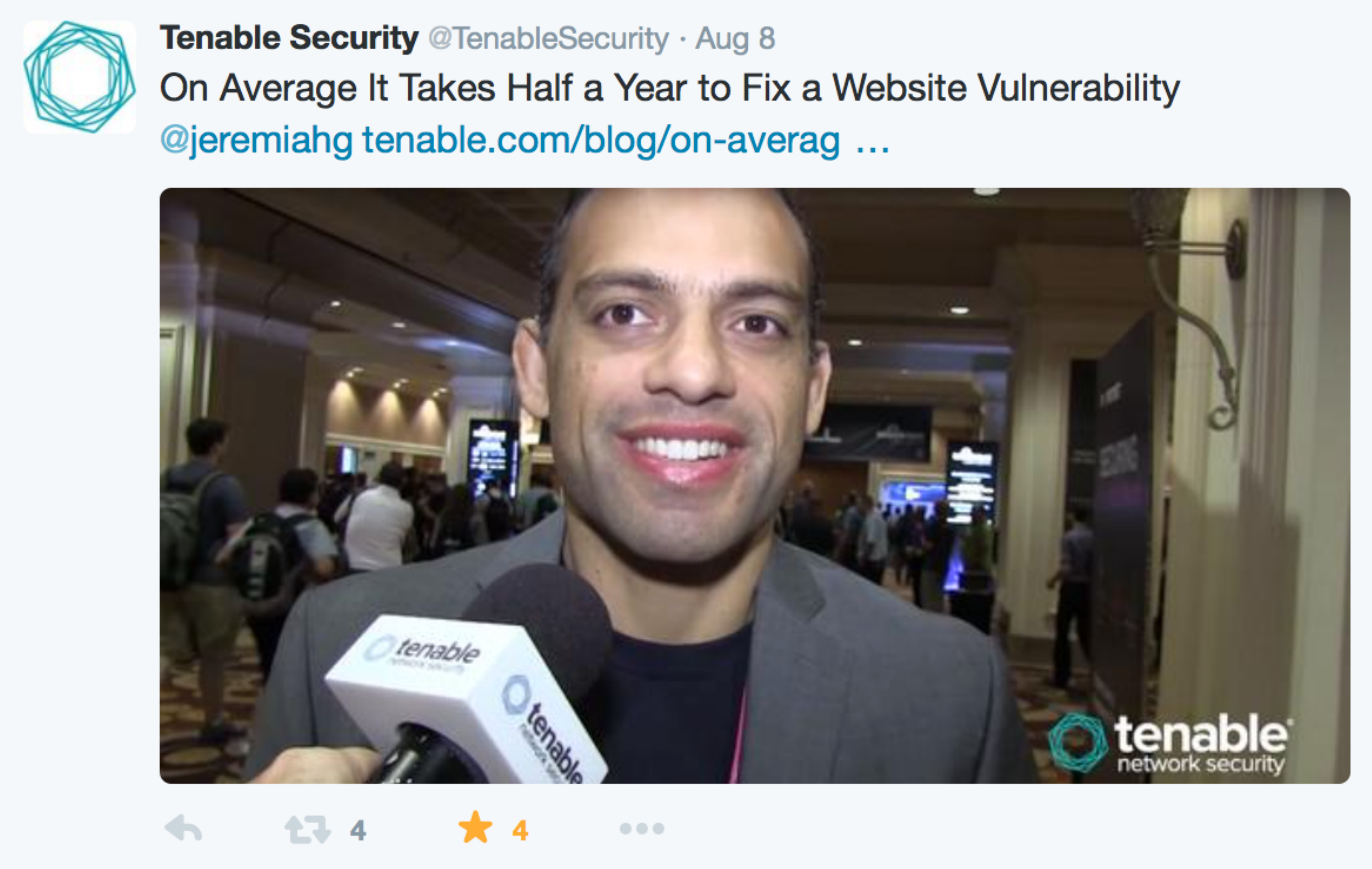
Software Safety issues are Security Issues

Getting Your Code To Production

Every engineering organization in the world is trying to go faster by using cloud, devops, continuous integration, agile

Or Planning To Do So, With Some Projects

Average time to fix a vulnerability is 150 days after being reported…. *you think that is due to technical reasons?*



Tenable Security @TenableSecurity · Aug 8

On Average It Takes Half a Year to Fix a Website Vulnerability @jeremiahg tenable.com/blog/on-averag …

TL;DR on Continuous Deployment

Security can make patches as needed

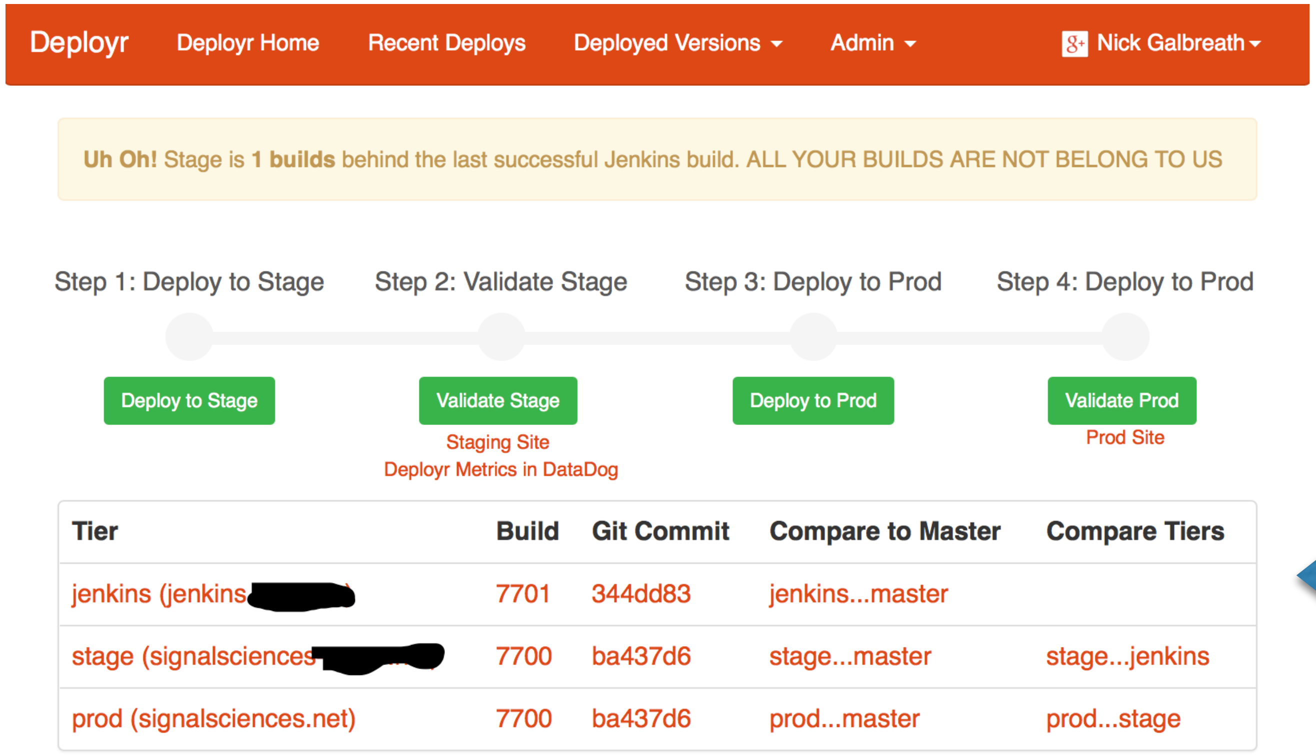
or

Require developers to do so in a timely manner

FOUND A NEW
VULNERABILITY
imgflip.com

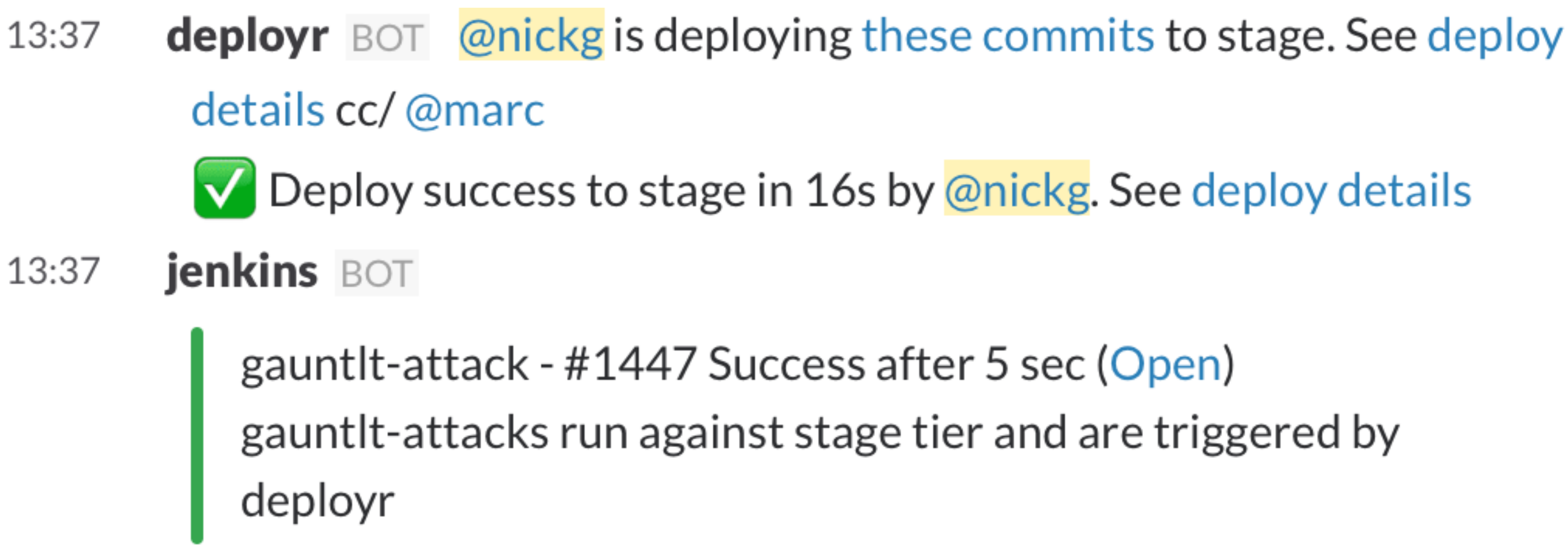
I DON'T ALWAYS FIND VULNS
BUT WHEN I DO, I PUSH THE FIX TO PRODUCTION
memegenerator.net

- ✓ Formatting Checks
- ✓ Linting
- ✓ Static Analysis
- ✓ Security Checks
- ✓ Unit Tests
- ✓ Integration Tests
- ✓ Spelling Checks
- ✓ Login / Auth



Uh Oh! Stage is **1 builds** behind the last successful Jenkins build. ALL YOUR BUILDS ARE NOT BELONG TO US

Tier	Build	Git Commit	Compare to Master	Compare Tiers
jenkins (jenkins[redacted]	7701	344dd83	jenkins...master	
stage (signalsciences[redacted]	7700	ba437d6	stage...master	stage...jenkins
prod (signalsciences.net)	7700	ba437d6	prod...master	prod...stage



13:37 **deployr** BOT @nickg is deploying these commits to stage. See deploy details cc/ @marc

✅ Deploy success to stage in 16s by @nickg. See deploy details

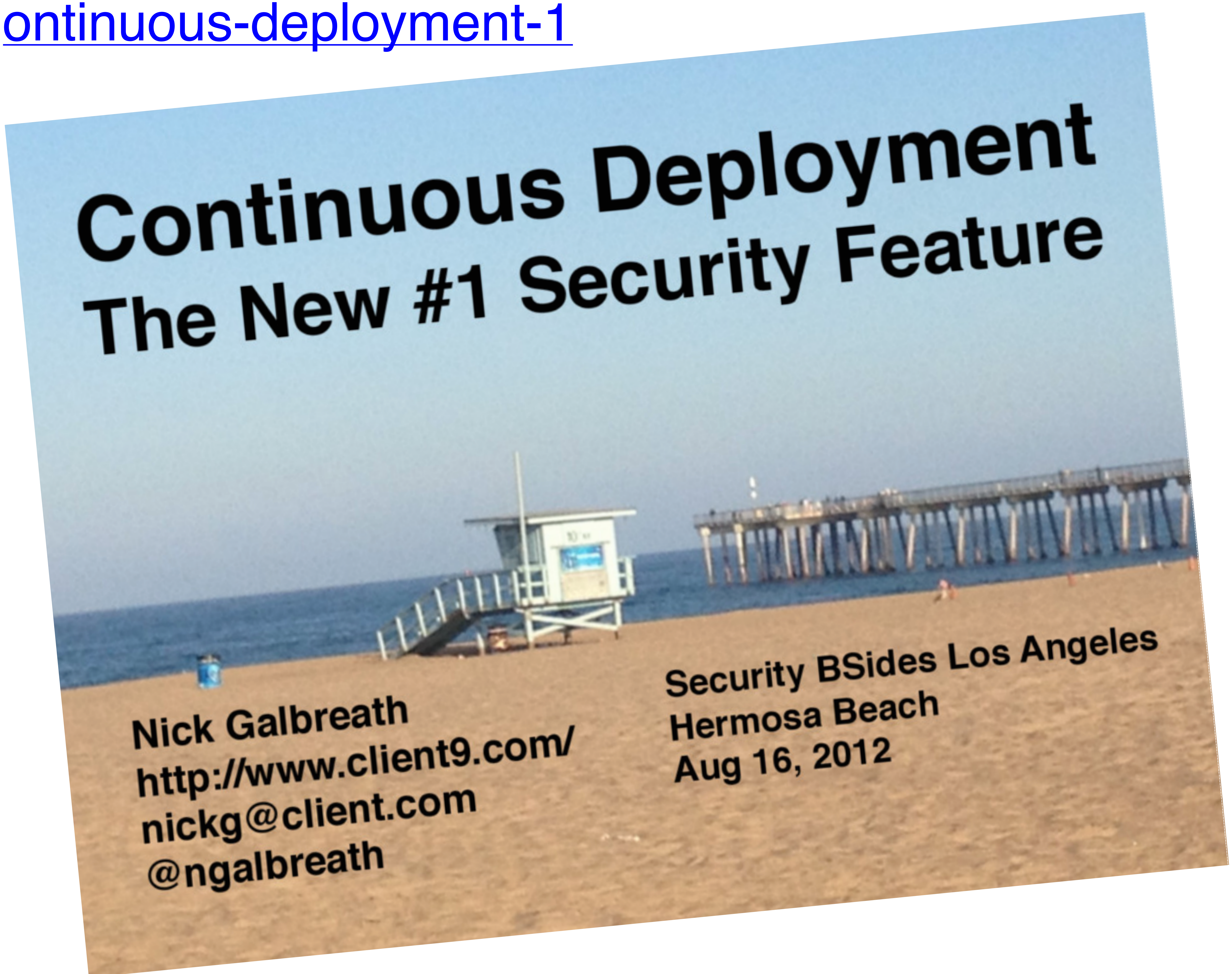
13:37 **jenkins** BOT

gauntlt-attack - #1447 Success after 5 sec (Open)
gauntlt-attacks run against stage tier and are triggered by deployr

How Code is Deployed is an Security Issue

Monitoring Your Code

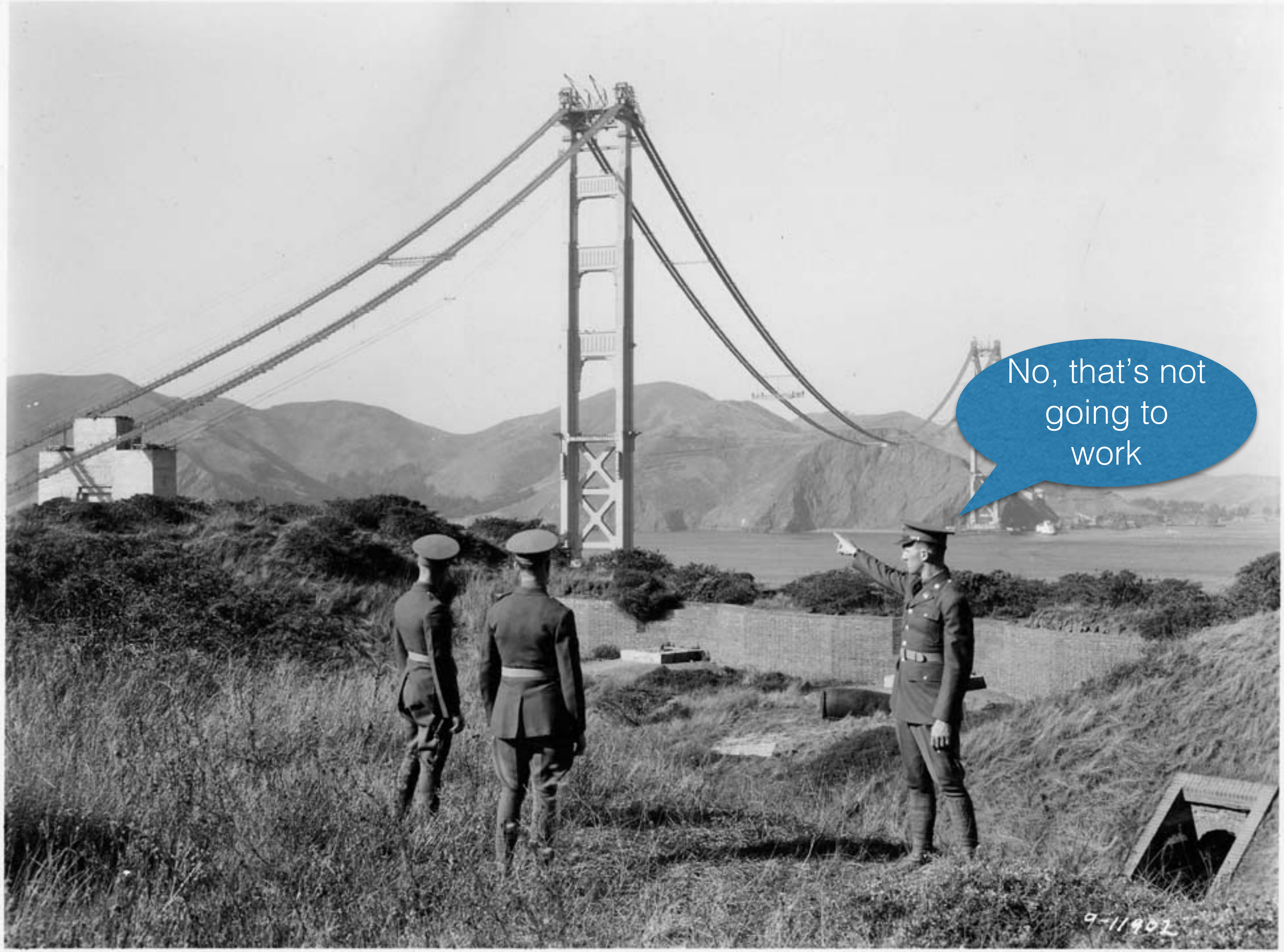
https://speakerdeck.com/ngalbreath/continuous-deployment-1



Continuous Deployment
The New #1 Security Feature

Nick Galbreath
http://www.client9.com/
nickg@client.com
@ngalbreath

Security BSides Los Angeles
Hermosa Beach
Aug 16, 2012



https://www.nps.gov/media/photo/gallery.htm?id=F865DA8A-155D-4519-3E66BBFECC74C707

Golden Gate NRA, Park Archives, Fort Point Photo Collection, GOGA-2042

Continuous Deployment Doesn't Change This Fact

👨👨👨👨👨👨👨👨👨👨

👨👨👨👨👨👨👨👨👨👨

👨👨👨👨👨👨👨👨👨👨

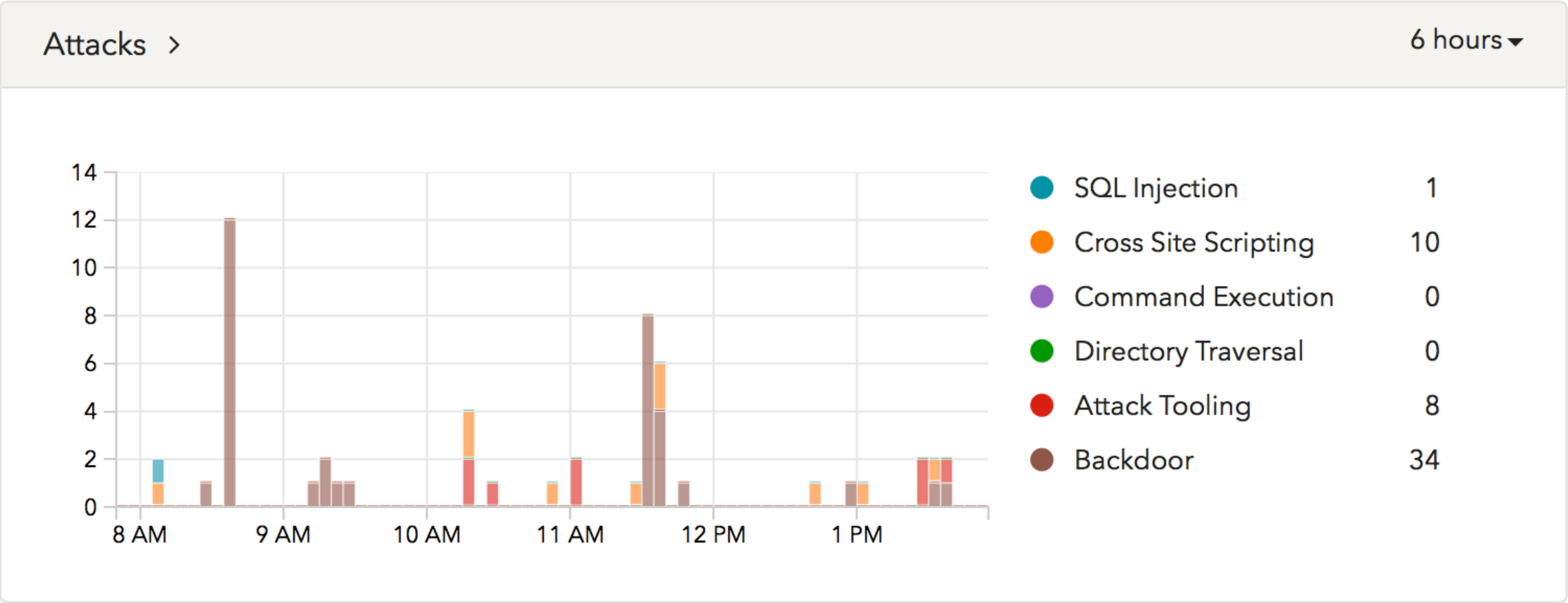
👨👨👨👨👨👨👨👨👨👨👨👨👨👨👨

👨👨👨👨👨👨👨👨👨👨👨👨👨👨👨😱

<vendor>

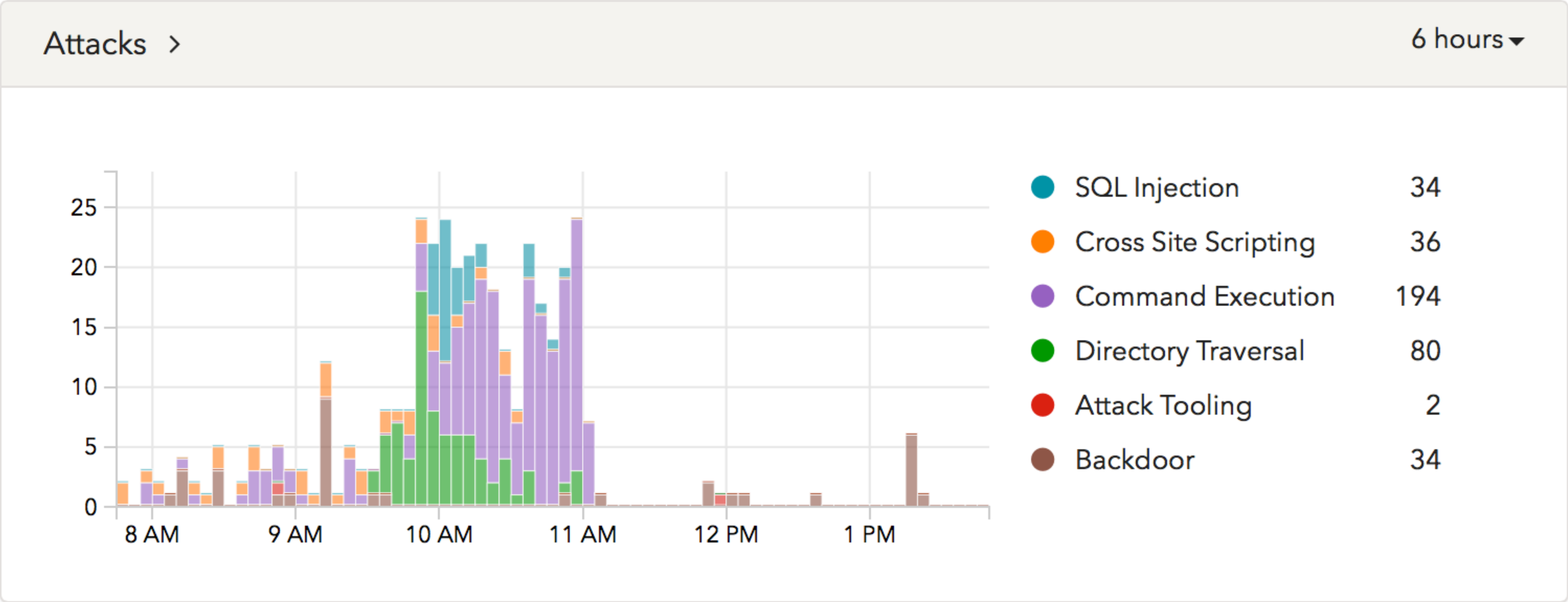
Very old screenshots

Cosmic Background Noise of Attacks



●	SQL Injection	1
●	Cross Site Scripting	10
●	Command Execution	0
●	Directory Traversal	0
●	Attack Tooling	8
●	Backdoor	34

Cloud-based scanner

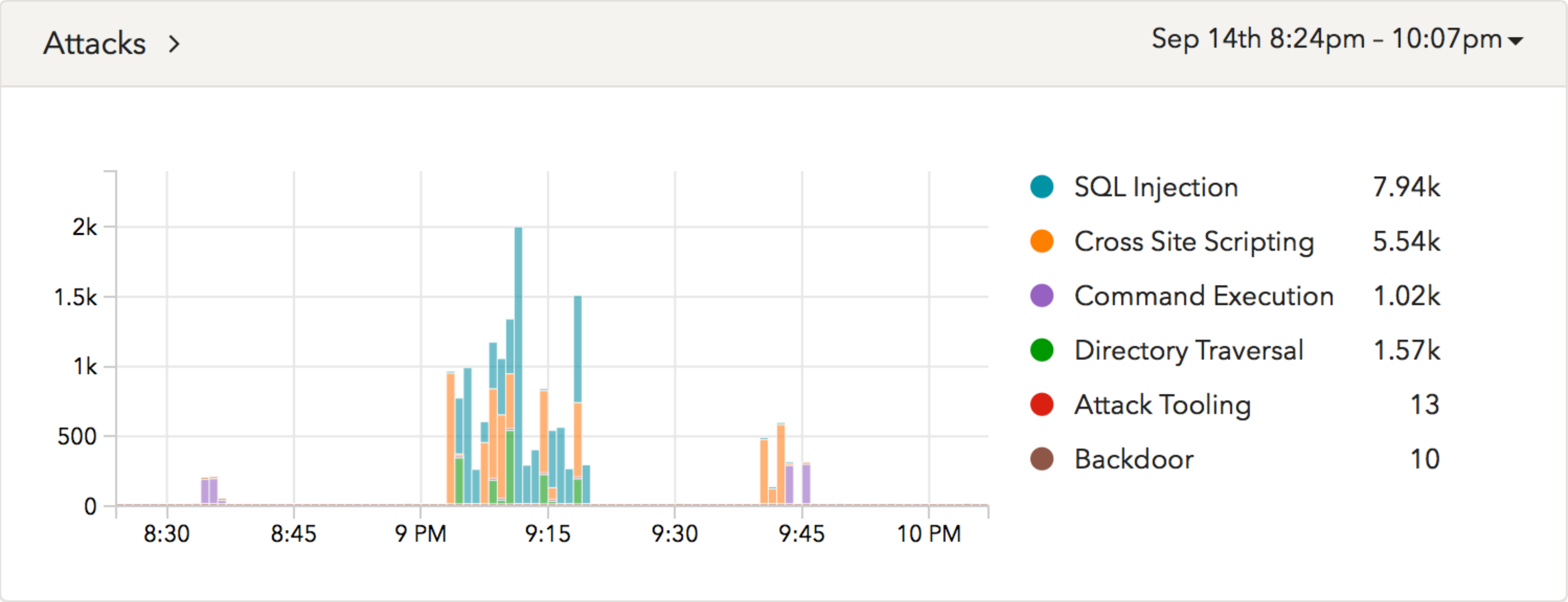


Attacks ›

6 hours ▾

●	SQL Injection	34
●	Cross Site Scripting	36
●	Command Execution	194
●	Directory Traversal	80
●	Attack Tooling	2
●	Backdoor	34

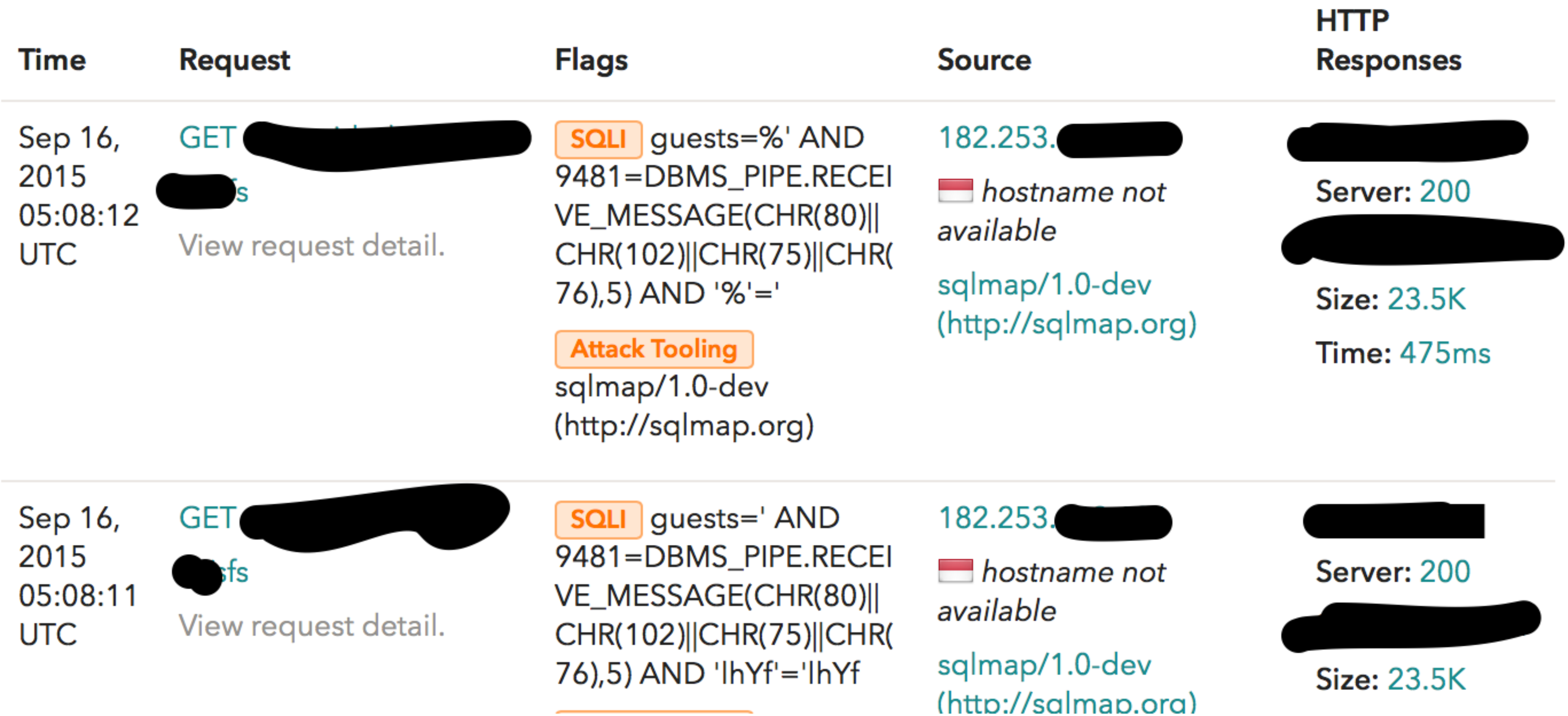
Attack Tooling



Attacks >

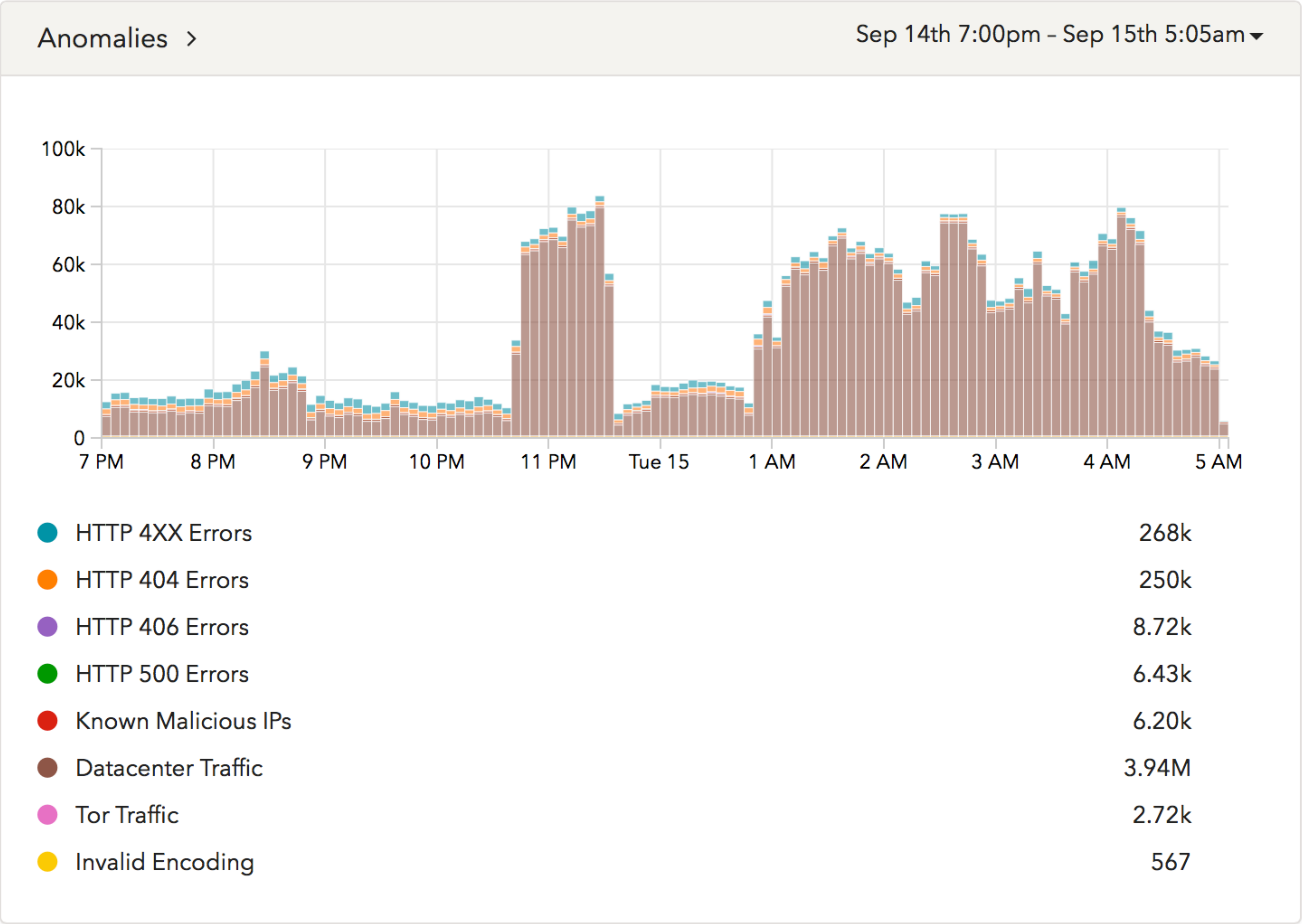
Sep 14th 8:24pm - 10:07pm ▾

●	SQL Injection	7.94k
●	Cross Site Scripting	5.54k
●	Command Execution	1.02k
●	Directory Traversal	1.57k
●	Attack Tooling	13
●	Backdoor	10



Time	Request	Flags	Source	HTTP Responses
Sep 16, 2015 05:08:12 UTC	GET [redacted] [redacted]s View request detail.	SQLI guests=%' AND 9481=DBMS_PIPE.RECEIVE_MESSAGE(CHR(80)||CHR(102)||CHR(75)||CHR(76),5) AND '%'=' Attack Tooling sqlmap/1.0-dev (http://sqlmap.org)	182.253.[redacted] *hostname not available* sqlmap/1.0-dev (http://sqlmap.org)	[redacted] Server: 200 [redacted] Size: 23.5K Time: 475ms
Sep 16, 2015 05:08:11 UTC	GET [redacted] [redacted]fs View request detail.	SQLI guests=' AND 9481=DBMS_PIPE.RECEIVE_MESSAGE(CHR(80)||CHR(102)||CHR(75)||CHR(76),5) AND 'lhYf'='lhYf	182.253.[redacted] *hostname not available* sqlmap/1.0-dev (http://sqlmap.org)	[redacted] Server: 200 [redacted] Size: 23.5K

Using SQLMap, on this URL, focused on 'guests'



Anomalies >

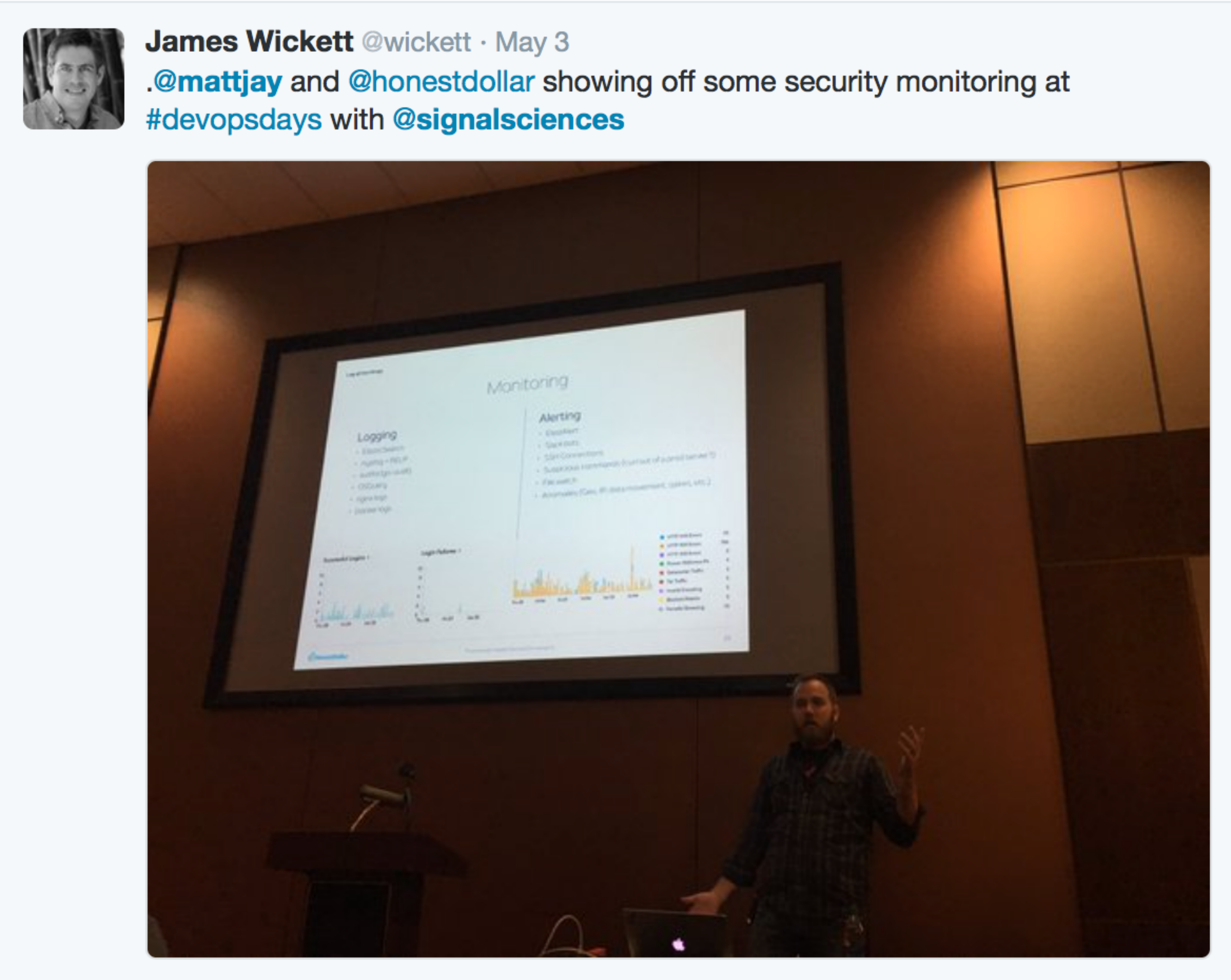
Sep 14th 7:00pm - Sep 15th 5:05am ▾

● HTTP 4XX Errors	268k
● HTTP 404 Errors	250k
● HTTP 406 Errors	8.72k
● HTTP 500 Errors	6.43k
● Known Malicious IPs	6.20k
● Datacenter Traffic	3.94M
● Tor Traffic	2.72k
● Invalid Encoding	567

</vendor>

Most Developers Have Never Seen
An Actual Attack on Their Code.
Any code.

It Changes Things



James Wickett @wickett · May 3

.@mattjay and @honestdollar showing off some security monitoring at #devopsdays with @signalsciences

Realtime
Application Monitoring
is a
Security Issue

When Your Code Fails

Breach Happens

There Will Be ~~Blood~~
Email

You Never Send Email to All Your Customers

- Marketing emails are done by another group/system, and have opt-outs. Might even have non customers in the list.

- Billing emails are staggered, and done by different group. And only if they have a bill.

- Other notifications are done “on demand” in real-time.

Let’s Do The Math

- Using your API gateway, maybe you are sending 1 email per second.

- That is ~12 days per million customers.

Assuming

- You can get the email list in the first place
- That your API provider doesn’t rate limit you due to massive change in volume
- That the email provider isn’t marking everything as spam.
- That your website doesn’t crash based on increase in logins due to your email.
- That your email sending process isn’t interrupted (need to mark who got an email)

Really?

- Ok, it’s unlikely Engineering is going to reprioritize the email stack just for this.
- But what is the IR plan?
- Does Engineering understand what it means?
- What is going to be the impact on CI?

Operational Infrastructure is a Security Issue.

Summary

These are Security Issues

- Where software comes from
- How software is written
- How software is deployed
- How software is monitored
- Software performance

Every Item Mentioned
Makes Engineering Better.
And more secure.

Start the Dialog

Can we make AppSec look more like this?

👨👨👨😱👨👨👨👨👨👨

👨👨👨👨👨👨👨👨😱👨

👨😱👨👨👨👨👨👨👨👨

👨👨👨👨👨😱👨👨👨👨😱👨👨👨👨

👨👨👨👨👨👨👨👨👨👨👨👨😱👨👨😱

Can’t Make an Impact?

0% Unemployment

Signal Sciences

nickg@signalsciences.com