

# Rugged Software Engineering

*Nick Galbreath @ngalbreath*  
Founder / CTO Signal Sciences



@ngalbreath  
#gotoldn

## Click 'engage' to rate session.

Rate **12** sessions to get the  
supercool GOTO reward



# Rugged Software Engineering

Nick Galbreath @ngalbreath  
Founder / CTO Signal Sciences



goto; conference - International Software Development - London 2015

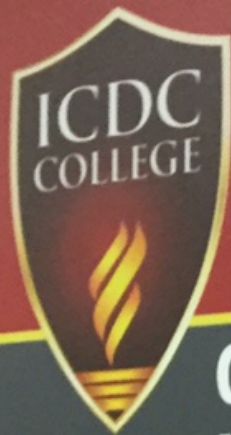












# CHANGE YOUR LIFE TODAY WITH A NEW CAREER

## GET JOB-READY IN A MATTER OF MONTHS!

**TRAIN FOR:**

- Homeland Security & Investigation
- Medical Assistant
- Physical Therapy Aide
- Web Developer
- Alcohol & Drug Counseling
- HVAC (Heating, Ventilation & Air Conditioning) Technician

■ NO HIGH SCHOOL DIPLOMA REQUIRED



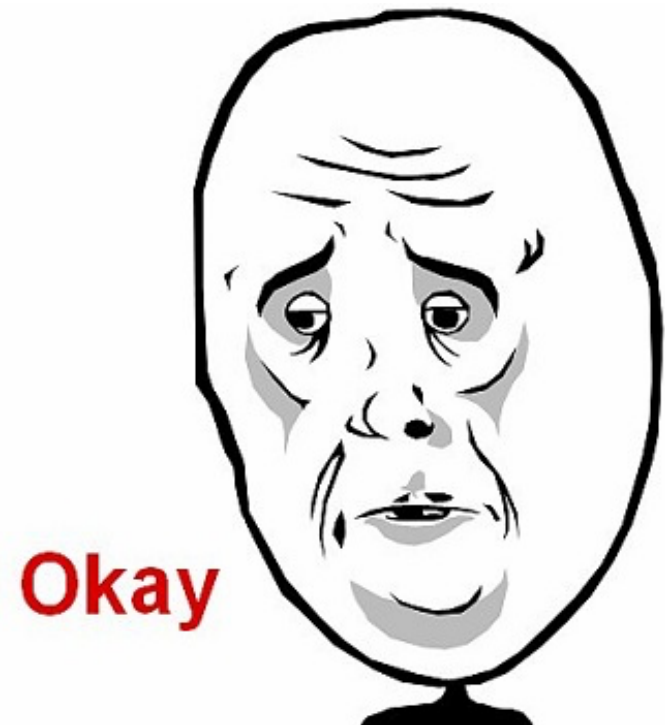


# Software Engineering





Technology concerned  
with the design, building  
and use of software



Software Engineering  
is not computer science







Software Engineering  
is not coding





Software Engineering  
is all of us

[Subscribe](#) | [Sign In](#)

256



11661



ESSAY

# Why Software Is Eating The World

By **MARC ANDREESSEN**

August 20, 2011

This week, Hewlett-Packard (where I am on the board) announced that it is exploring jettisoning its struggling PC business in favor of investing more heavily in software, where it sees better potential for growth. Meanwhile, Google plans to buy up the cellphone handset maker Motorola Mobility. Both moves surprised the tech world. But both moves are also in line with a trend I've observed, one that makes me optimistic about the

# World to Software: Right back at you.

Crime

Politics

Regulation

Liability

Ethics

Money



# Software Liability is Inevitable



Jeff Moss, Black Hat USA 2015

<http://techcrunch.com/2015/08/06/should-software-companies-be-legally-liable-for-security-breaches/>  
<https://threatpost.com/software-liability-is-inevitable/114136/>

I think we're going to do a really crappy job with software liability for a long time, and the people who will suffer will be the innovators and the startups, not the established companies

Jennifer Granick,  
Black Hat USA 2015 Keynote  
2015-08-04 around minute 46:00  
[https://www.youtube.com/watch?v=Tjvw5fz\\_GuA](https://www.youtube.com/watch?v=Tjvw5fz_GuA)



## National Security

# Insurance requirements can drive stronger cybersecurity, Treasury official says

The market for cyber insurance began to take off about five years ago, Beshar said. Today, globally, **about \$2 billion worth of premiums have been sold.** Most of that coverage is in the United States, but the market is growing substantially, he said.

2015-09-10

<http://wapo.st/1gcDU9i>



Home > News > 'Featured' > Senate Introduces Automotive Anti-Hacking Bill

# ***Senate Introduces Automotive Anti-Hacking Bill***

July 21, 2015 at 3:40 pm by **Clifford Atiyeh** | Photography by **Chip Somodevilla/Getty Images**



***... the bill wants automakers to establish real-time monitoring to “immediately detect, report, and stop” hacking attempts in their cars.***

# (USA) Government ranks last in fixing software security holes

Three-quarters of all government Web and mobile  
applications fail their initial security reviews

CSO Online / Veracode  
Jun 23, 2015

... and then only fixing 27% a year later

<http://www.csoonline.com/article/2939234/application-security/government-ranks-last-in-fixing-software-security-holes.html>



# Online marauders States use hackers to do cyber dirty work

SAM JONES — LONDON

A new breed of sophisticated hacker is emerging as one of the most worrisome digital adversaries for western intelligence chiefs — cyber privateers.

Just as England's Elizabeth I officially licensed pirates to plunder the treasure ships of her rival Philip II of Spain in the 16th century, nations such as Russia and Iran are increasingly arming and encouraging criminal and activist groups with cyber weaponry, while keeping themselves at arms length, senior security and defence officials in the US and Europe believe.

"A lot of the techniques that were the preserve of state sponsored attackers are starting to make their way into broader communities of criminals," says Simon Goldsmith at Applied Intelligence, the cyber unit of defence contractor BAE System.

"It is proliferating in a massive way and the object of attacks by these groups is moving from large financial theft to using the same techniques to commit sabotage and for intelligence gathering."

State use of proxy agents to carry out disguised attacks is not new but a shift has occurred in recent months, with a dramatic increase in the sophistication and number of worrisome attacks from non-state groups, western security officials have told the Financial Times. They point to a handful of serious attacks in which proxy organisations or criminal groups appear to have played a central role, with a nation state agency working in the background.

When Sony Pictures was hacked late last year, the US government confidently attributed the attack to Pyongyang. However, several follow-up incidents may not have been from North Korea, even though they were disguised to appear as though they were state sponsored. Officials say cyber pri-



**Financial Times 2015-09-15**  
**<http://on.ft.com/1PQnM9H>**

ingly unclear," says Ewan Lawson, senior research fellow at the UK's Royal United Services Institute and a former cyber warfare officer at the UK's Joint Forces Command. "What is happening is that adversaries are turning to these peripheral groups and saying 'here's a list of areas we are happy for you to go into and here are some tools to do it'. It is a charter to hack."

A tell-tale sign comes from tracing the "DNA" of pieces of malware — the malicious software used in attacks. Disentangling the evolution of such cyber-weapons is nevertheless tricky: while criminals could have been given them by government agencies, they could also have copied them malware already in use.

**"The object is to use the same techniques to commit sabotage and for intelligence gathering"**

One of the greatest concerns around the rise of cyber privateering is that once criminal groups have been equipped with the ability to penetrate well-defended organisations such as foreign government agencies or utilities, there may be little to stop them from later turning their attention to other, more lucrative targets.

Officials also worry about their propensity to slip up, or overstep the mark. "They are generally more dangerous because they don't necessarily have the situational awareness to moderate their impact," said one western security official.

As nations such as the US grow more confident in attributing — and retaliating to — attacks, most expect their adversaries in cyber space to ramp up their use of privateer agents.







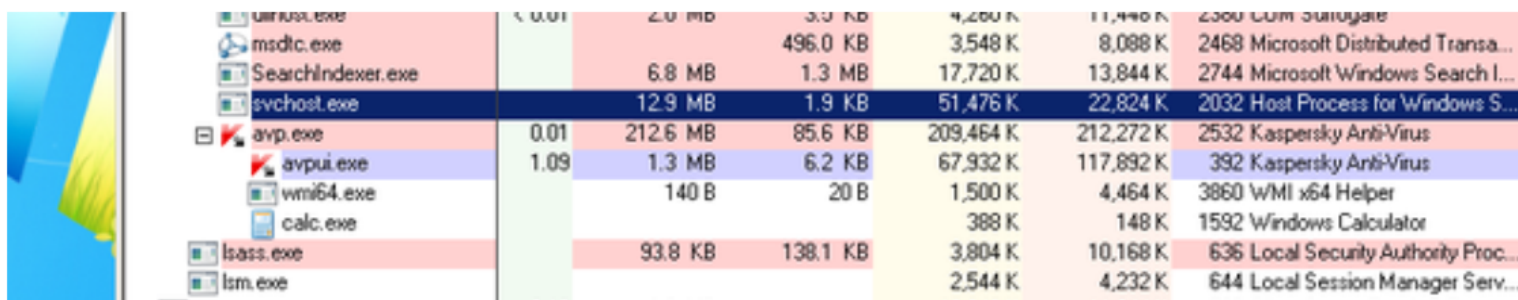
**Tavis Ormandy**

@taviso



Follow

Okay, first Kaspersky exploit finished, works great on 15 and 16. Will mail report after dinner. /cc @ryanaraine



explorer.exe	0.01	2.0 MB	3.0 KB	4,260 K	11,440 K	2360	COM Surrogate
msdtc.exe			496.0 KB	3,548 K	8,088 K	2468	Microsoft Distributed Transa...
SearchIndexer.exe		6.8 MB	1.3 MB	17,720 K	13,844 K	2744	Microsoft Windows Search I...
svchost.exe		12.9 MB	1.9 KB	51,476 K	22,824 K	2032	Host Process for Windows S...
avp.exe	0.01	212.6 MB	85.6 KB	209,464 K	212,272 K	2532	Kaspersky Anti-Virus
avpui.exe	1.09	1.3 MB	6.2 KB	67,932 K	117,892 K	392	Kaspersky Anti-Virus
wmi64.exe		140 B	20 B	1,500 K	4,464 K	3860	WMI x64 Helper
calc.exe				388 K	148 K	1592	Windows Calculator
lsass.exe		93.8 KB	138.1 KB	3,804 K	10,168 K	636	Local Security Authority Proc...
lsm.exe				2,544 K	4,232 K	644	Local Session Manager Serv...



**Tavis Ormandy** @taviso · Sep 5

@ryanaraine It's a remote, zero interaction SYSTEM exploit, in default config. So, about as bad as it gets.

<https://twitter.com/taviso/status/639992212164513792>

Note: Patched and pushed in a day. Excellent



<https://twitter.com/h3rm4ns3c/status/638940105529499648>

Are you kidding me.

# 44CON LONDON

IT Security Conference  
9th to 11th September 2015

ILEC Conference Centre

IT Security Training Event  
7th to 9th plus 14th & 15th

[https://www.ernw.de/download/  
ERNW\\_44CON\\_PlayingWithFire\\_signed.pdf](https://www.ernw.de/download/ERNW_44CON_PlayingWithFire_signed.pdf)

**COMPUTERWORLDUK**

THE VOICE OF IT MANAGEMENT

Technology

News

Features

IT Business

## FireEye takes security firm to court over vulnerability disclosure

*By Jeremy Kirk | IDG News Service | Published 04:59, 11 September 15*



# LAW & DISORDER / CIVILIZATION & DISCONTENT

## Pwn2Own loses HP as its sponsor amid new cyberweapon restrictions

Concerns about violating international arms treaty behind pull-out.

by **Dan Goodin** - Sep 3, 2015 4:57pm CEST

 [Share](#)

 [Tweet](#)

34

The next scheduled Pwn2Own hacking competition has lost Hewlett-Packard as its longstanding sponsor amid legal concerns that the company could run afoul of recent changes to an international treaty that governs software exploits.

Dragos Ruiu, organizer of both Pwn2Own and the [PacSec West](#) security conference in Japan, said HP lawyers spent more than \$1 million researching the recent changes to the so-called Wassenaar Arrangement. He said they ultimately concluded that the legal uncertainty and compliance hurdles were too high for them to move forward.



**Dan Guido** @dguido · Sep 11

Let this be another data point for software security: 16 yrs old, little to no prior security exp, 6 weeks has her first 0day fully analyzed



48



50



[View conversation](#)



**Dan Guido** @dguido · Sep 11

If any of you caught our HS intern on Twitter the other week, here's the full writeup of what she did this summer:

[blog.trailofbits.com/2015/09/10/sum...](http://blog.trailofbits.com/2015/09/10/sum...)



51



74



[View summary](#)



Dan Guido retweeted

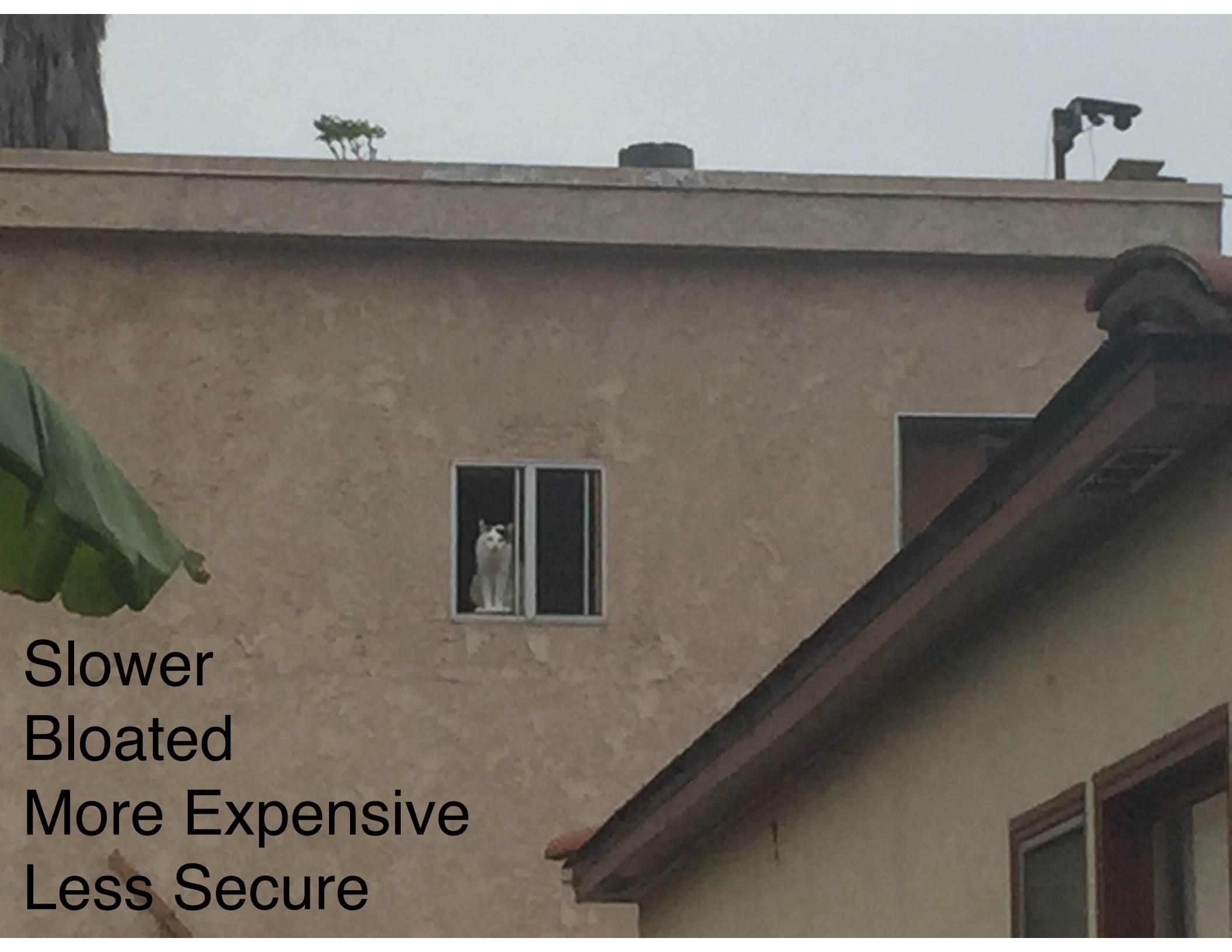
**CVE-2015-5949**



**Trail of Bits** @trailofbits · Sep 10

Summer @ Trail of Bits [blog.trailofbits.com/2015/09/10/sum...](http://blog.trailofbits.com/2015/09/10/sum...)






Slower  
Bloated  
More Expensive  
Less Secure



# What Went Wrong?





A large, dark wood bookshelf with a grid-like structure. Most of the shelves are empty. In the middle-right section, there is a small stack of books on one shelf, a small black box on the shelf below it, and a clear plastic water bottle on the shelf below that. The bottom of the unit consists of four large, solid wood cabinet doors. The background is a plain, light-colored wall.

# Security is Invisible for Most of the Organization

Invisible Things Aren't Valued



A detailed mosaic of Medusa's head, the Gorgon, surrounded by a circular border and radiating lines, set against a background of dark, wavy patterns.

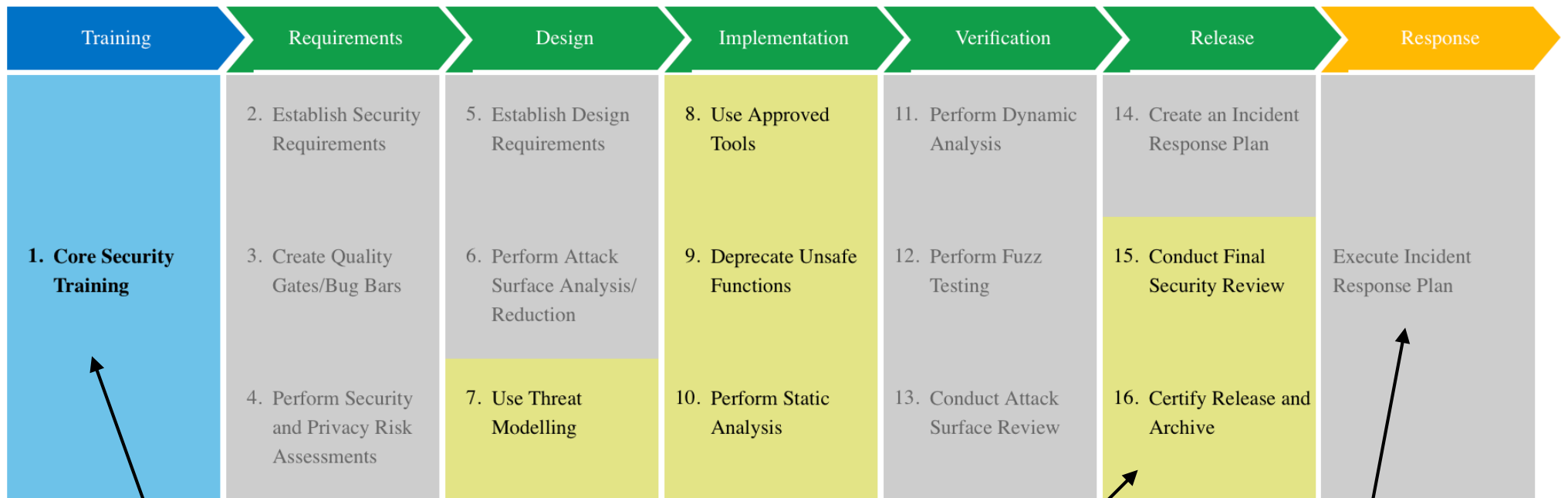
# **100-10-1 Ratio Waterfall Model**

**You can not hire out of this**



# SDLC?

<http://www.microsoft.com/en-us/SDL/Discover/sdlagile.aspx>



Send the devs to  
Security Camp once a year

deploy  
incident response  
disconnected from dev





**OJ**

@TheColonial



**Follow**

I'm yet to see a company admit that they got owned because of a typical flaw in their security, not through "a sophisticated attack".

---

<https://twitter.com/TheColonial/status/642199904547307520>

failing at easy stuff.

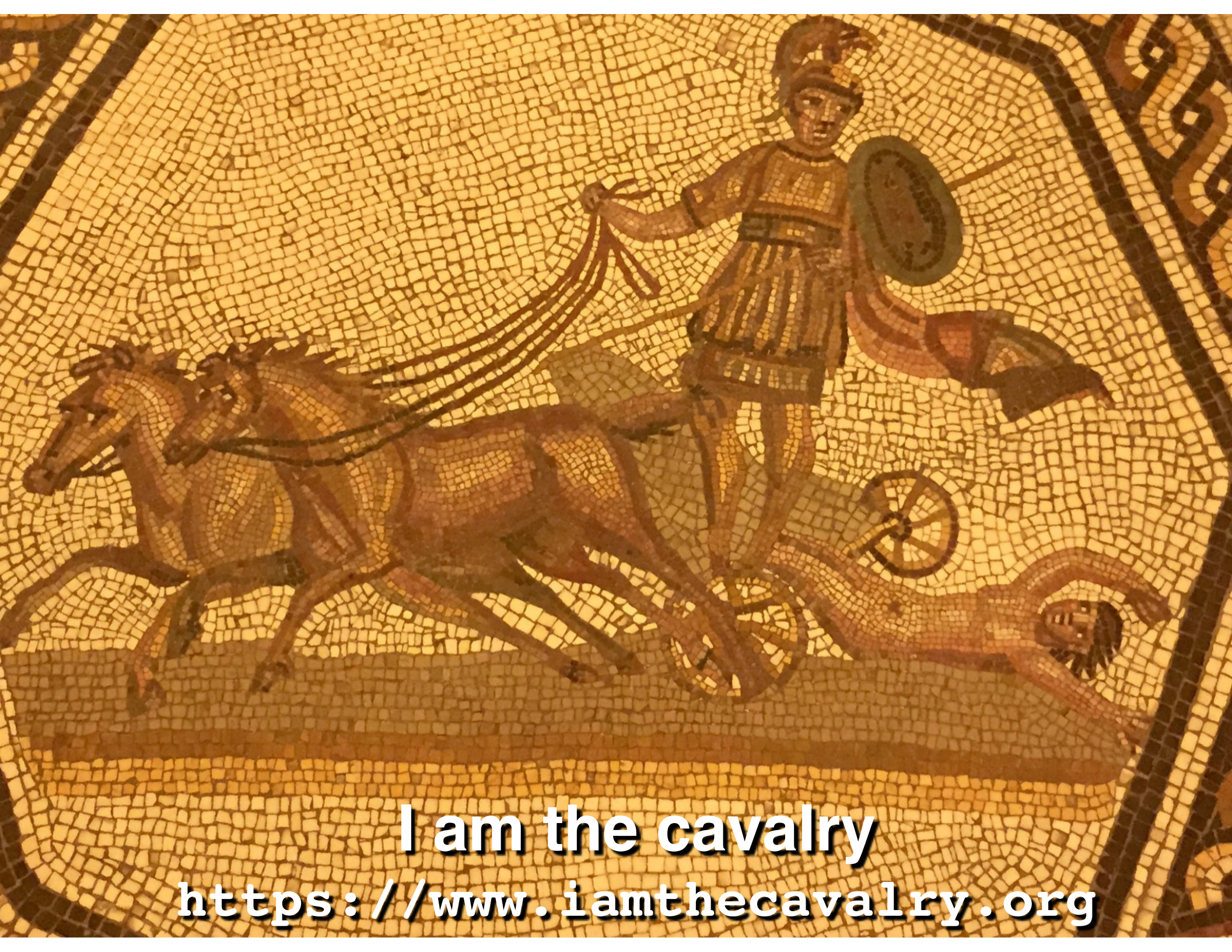
---

## HOUSE SPECIALS!

### **Canal Club Sashimi Pizza**

Truffle Aioli, Dijon Ponzu, Micro Mix, Reed Onion, Fried  
Tortilla \$14.50





**I am the cavalry**

**<https://www.iamthecavalry.org>**





**We are the cavalry**



A close-up photograph of a cobblestone pavement. The stones are dark grey and irregularly shaped, set in a light-colored, sandy mortar. The word "Rugged" is overlaid in the center in a large, bold, black sans-serif font.

**Rugged**





Imperva @Imperva



Keep your headlines positive. Choose the proven leader in Web App Firewalls. #cybersecurity [ow.ly/M2tM3](https://ow.ly/M2tM3)



Promoted



10

42



Kaspersky Lab @kaspersky

3h

How does Kaspersky Internet Security protect you from #ransomware? - [ow.ly/NhSVc](https://ow.ly/NhSVc)





# Maybe Unfair Comparison

- Dynamic
- Risk-Based
- Continuous
- Cross-Team
- Hopefully appealing
- Static
- List-Based
- Discrete
- Single Team
- Tainted Word

Software development should be thought of as a cycle of continual learning and improvement rather a progression from start to finish, or a search for correctness.

@kellan 2015-08-31

<https://medium.com/@kellan/five-years-building-a-culture-and-handing-it-off-54a38c3ab8de>



Software  
Engineering  
is a  
Team Sport







building  
things  
together





But also, you have an  
*adversary.*



Cleaning up

PreDeploy  
Deploy  
PostDeploy





# Style Matters





**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.



1



3



**Colin Percival**

@cperciva



Following

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.bsdcn.org/2012/schedule/attachments/  
218\\_crowdsec.pdf](https://www.bsdcn.org/2012/schedule/attachments/218_crowdsec.pdf)

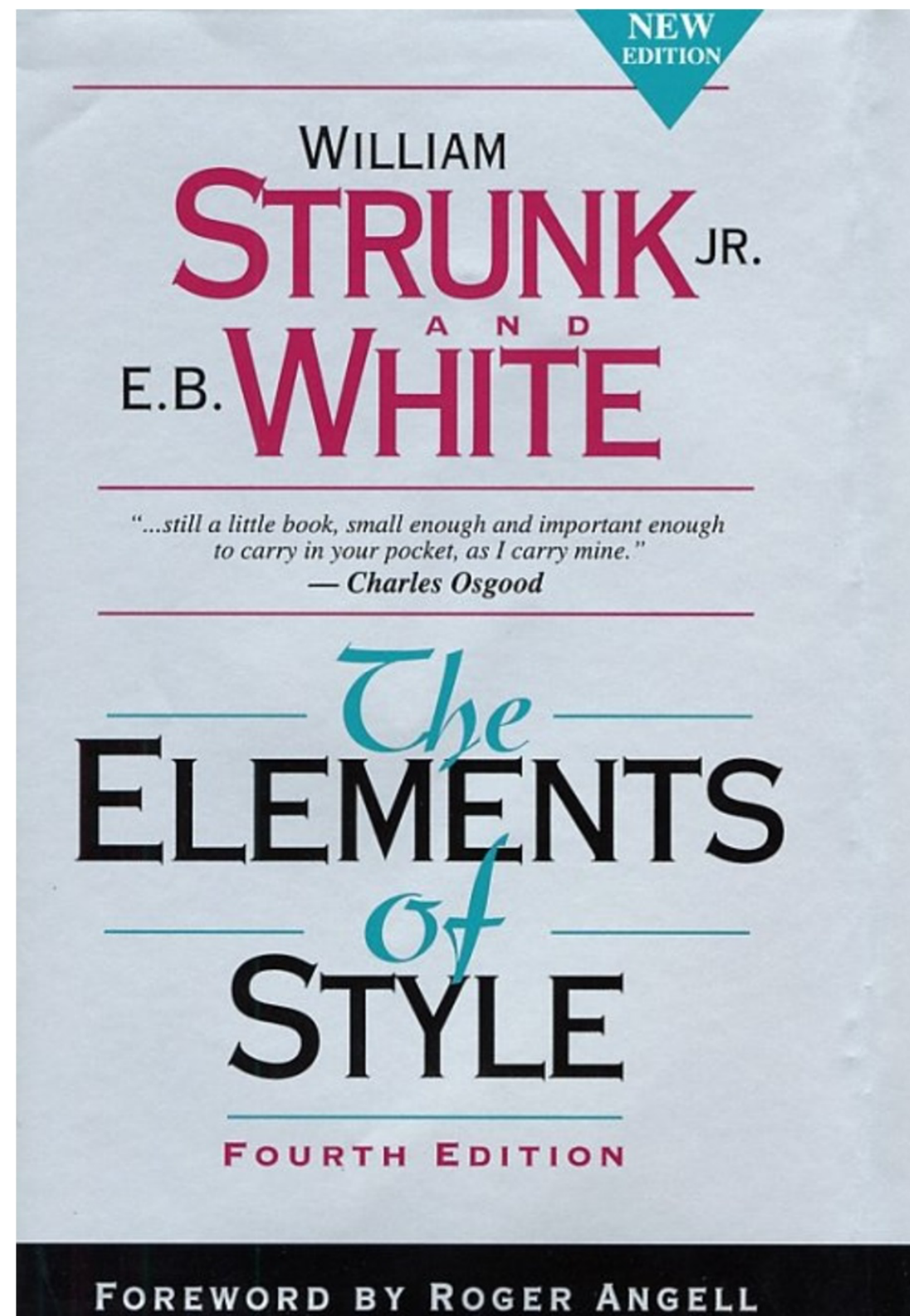
# The Buried Lead: 4x Faster Bug Fixes

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  $4 \times$  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.



# 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();  
>+}
```



**"ANCHE IL CORPO HA  
IL SUO LINGUAGGIO"**

**VESTI CON DIGNITÀ E  
RISPETTA IL LUOGO SACRO**

**È SCONVENIENTE UN ABBIGLIAMENTO  
SENZA MANICHE, IN MINIGONNA, IN PANTALONCINI**



E' VIET

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.



Broken windows theory - Wikipedia, the free encyclopedia

[https://en.wikipedia.org/wiki/Broken\\_windows\\_theory](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/evidence-based-policing/what-works-in-policing/research-evidence-review/broken-windows-policing/>



# 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.

# Static Analysis

- You are insane if you don't have automated static analysis running.
- The closer it can run to the developer the better (i.e. can they run it locally or in editor?)



# Security Testing?

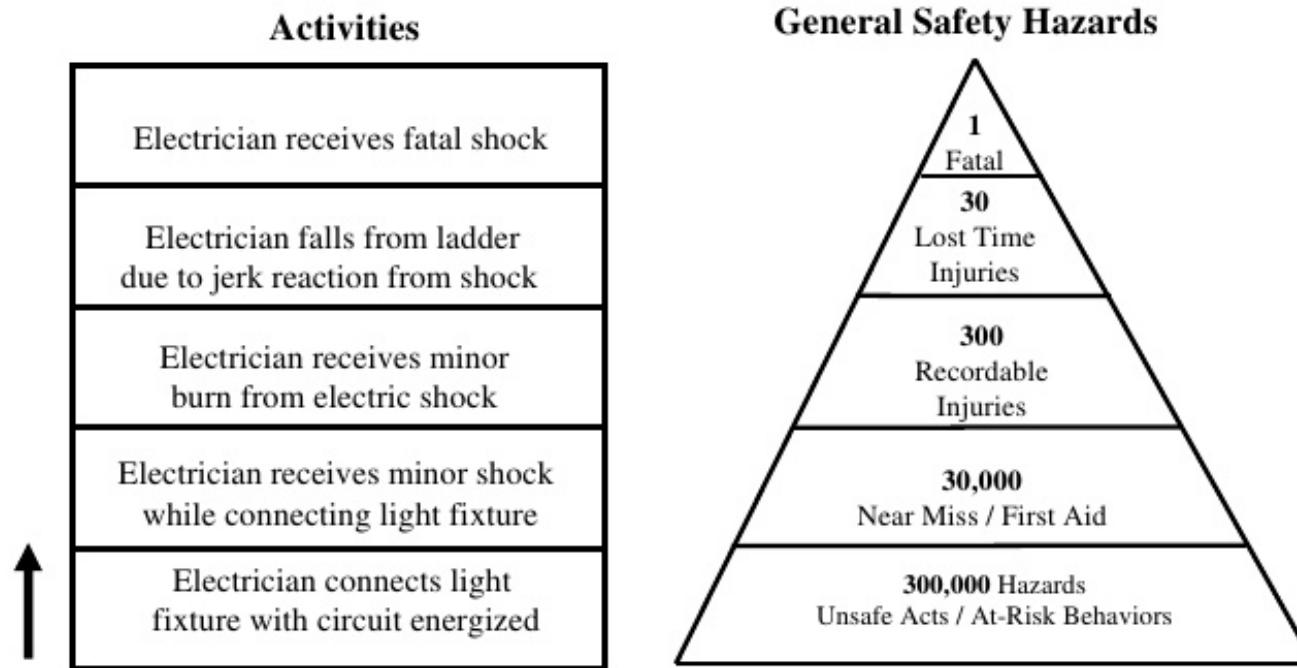
# OpenSSL Heartbleed



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



# HEINRICH THEORY



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

# Not just for the "software development team"

Ops: Puppet / Chef / Dockerfiles, etc

QA: testing patterns, cucumber

Everyone: configuration and glue



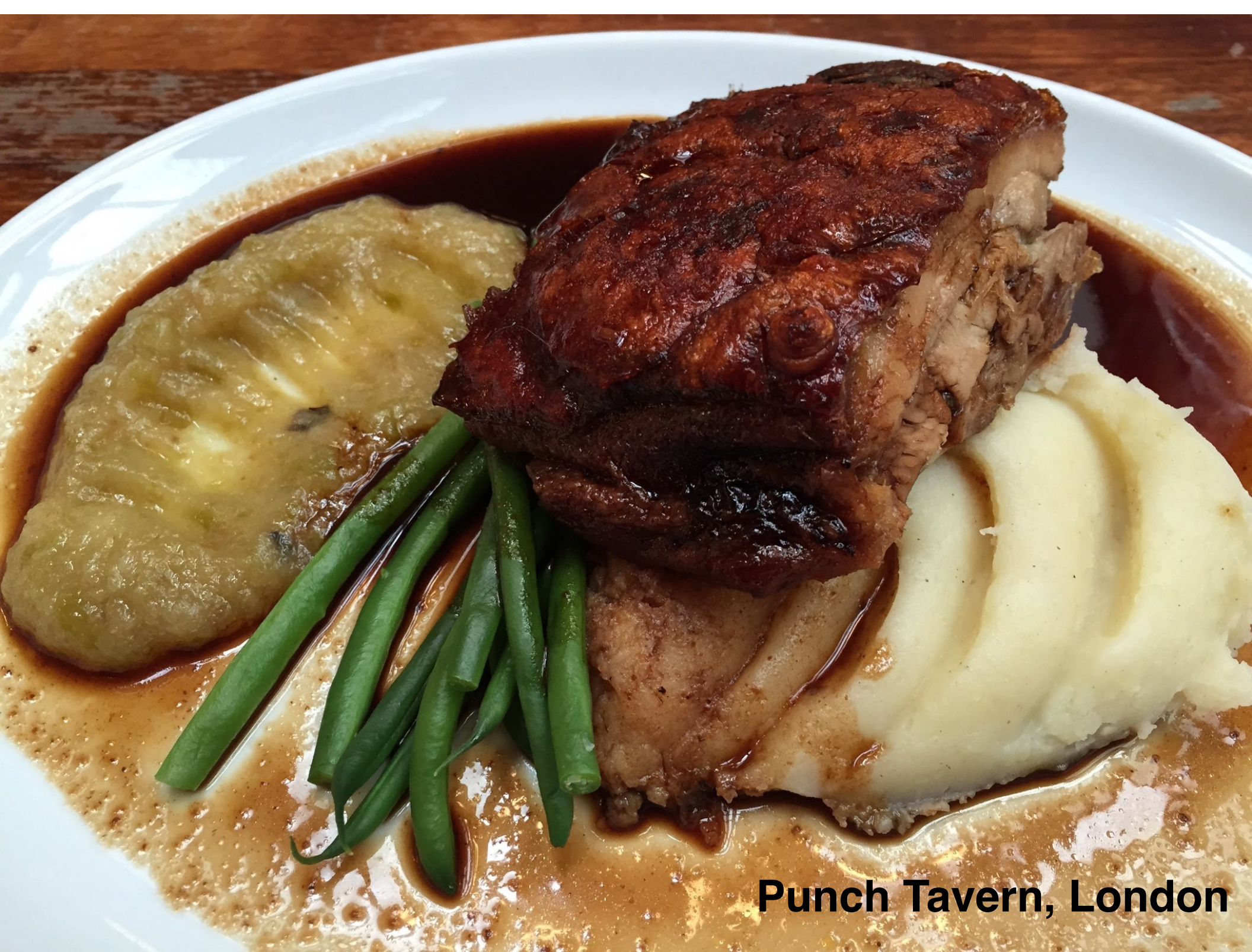
# Continuous Deployment

Formerly known as  
Release Engineering



"Alien" slot machine,  
Las Vegas  
2015-08





**Punch Tavern, London**





Smaller  
Chunks,  
More  
Often



Continuous meaning  
*fluid* not "all the time"





```
> function foobar() {...  
>...  
> }
```

```
// doco..  
> function foobar() {...  
>...  
> }  
  
> function test_foobar() {  
>     ...  
> }
```



```
$usenewstuff = false;
```

```
if ($usenewstuff) {  
    foobar();  
} else {  
    old_code();  
}
```

No: Update

Yes: Add, Then Delete





How often you deploy  
is your decision



**But when you do,  
it should be  
without ceremony**





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](https://tenable.com/blog/on-average) ...



4



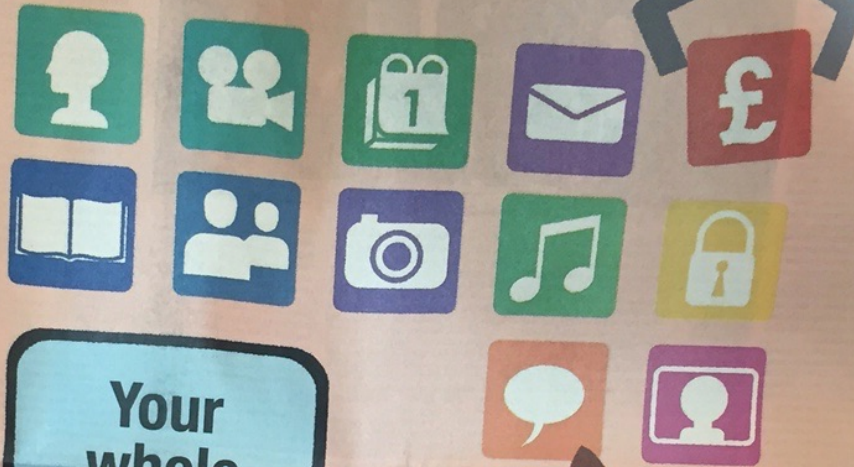
4





HM Government

# Don't Forget the Server!



Your  
whole  
life  
is here.  
Is it  
secure?

Software  
Update

Software updates contain vital security upgrades which help protect your device from viruses and hackers.

**Always download the latest software updates.**



# Continuous Deployment applies to your OS as well as your application

The CIOs surveyed named the top 3 common information system vulnerabilities as being related to application security (55%), security awareness (51%), **and, perhaps most surprisingly, out-of-date security patches (50%).**

<http://www.information-age.com/industry/software/123459579/why-your-business-cant-afford-not-patch>

2015-06-02



**Kaspersky Lab** @kaspersky · Sep 8

52% of all businesses surveyed regularly patch or update software.

Read more: [kas.pr/3xt7](http://kas.pr/3xt7) #ebook #infosec

Security folks have been reluctant to  
continuous deployment for the applications.

Love it for the OS\*

And application patches\*

Operations typically doesn't like deployment  
ever, OS or Application.\*

Developers love continuous deployment, but  
don't care about security or operations\*.

\* Your experience may differ



The background is a complex Baroque fresco. It features a dense crowd of figures, including men, women, and children, in various poses of movement and emotion. They are dressed in rich, colorful garments typical of the 17th century. The scene is set within a grand architectural space with large columns, arches, and a high ceiling. The overall composition is dynamic, with strong contrasts of light and shadow, characteristic of Baroque art. The text 'Runtime Security Monitoring' is superimposed in the center in a white, sans-serif font. The word 'Security' is italicized, while 'Runtime' and 'Monitoring' are in a standard weight. A small black dot is positioned to the left of the word 'Security'.

# Runtime *Security* Monitoring

# runtime monitoring

- machine level monitoring
- application level monitoring
- code-level monitoring
- but security monitoring?



# Key Questions

- What are the attacks (they are happening)
- Where are they attacking
- Are they being successful

And making this visible





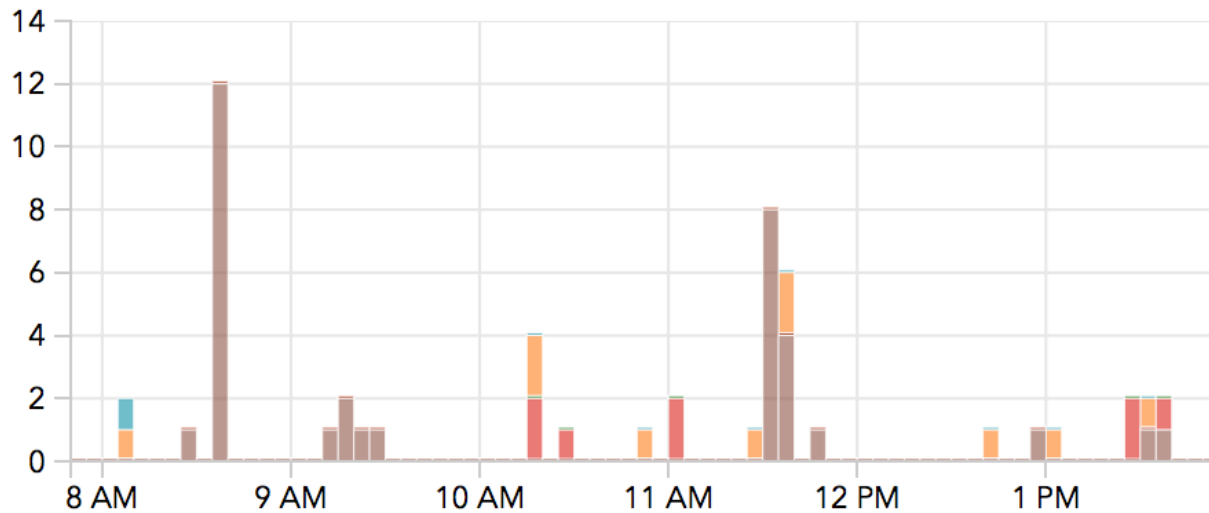
**Closing the feedback  
loop to developers**



# Cosmic Background Noise of Attacks

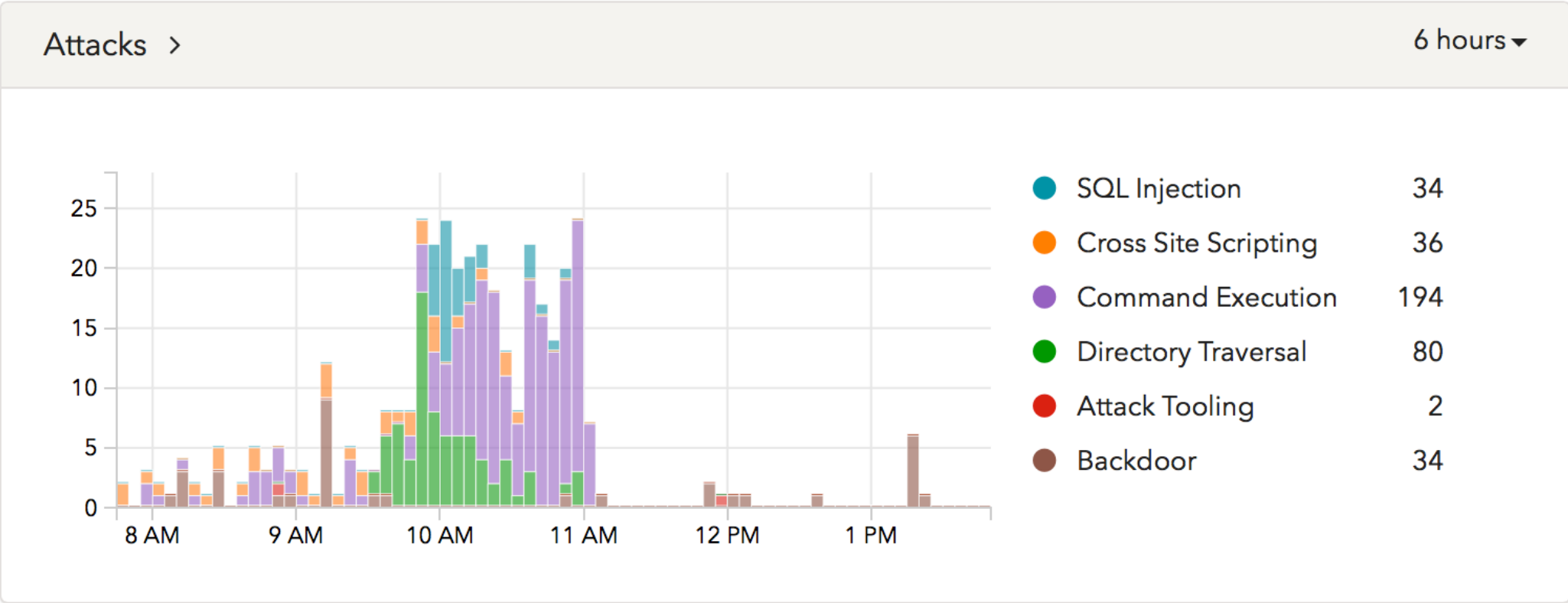
Attacks >

6 hours ▼



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

# Cloud-based scanner

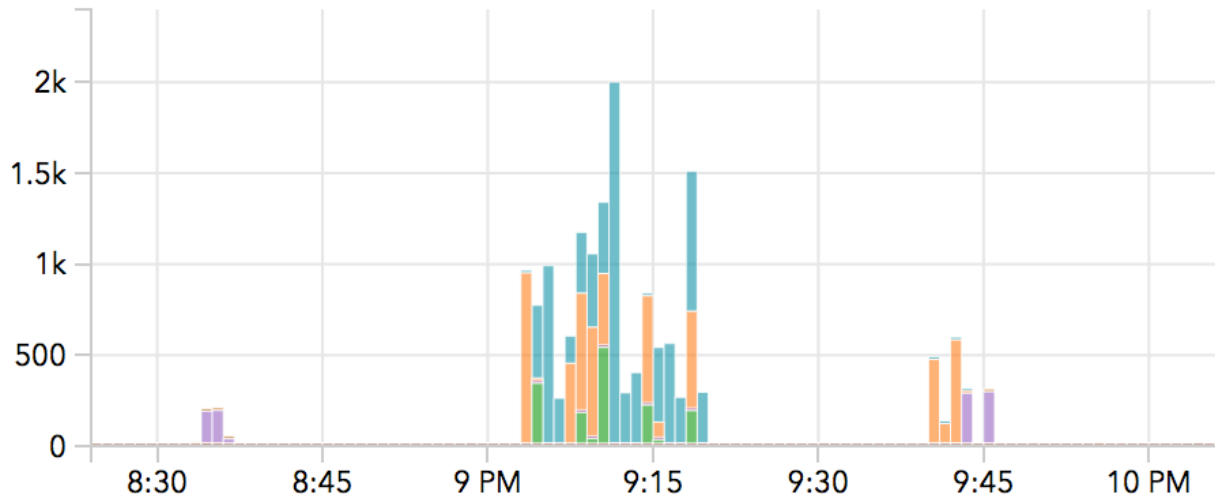




# Attack Tooling

Attacks >

Sep 14th 8:24pm - 10:07pm ▼

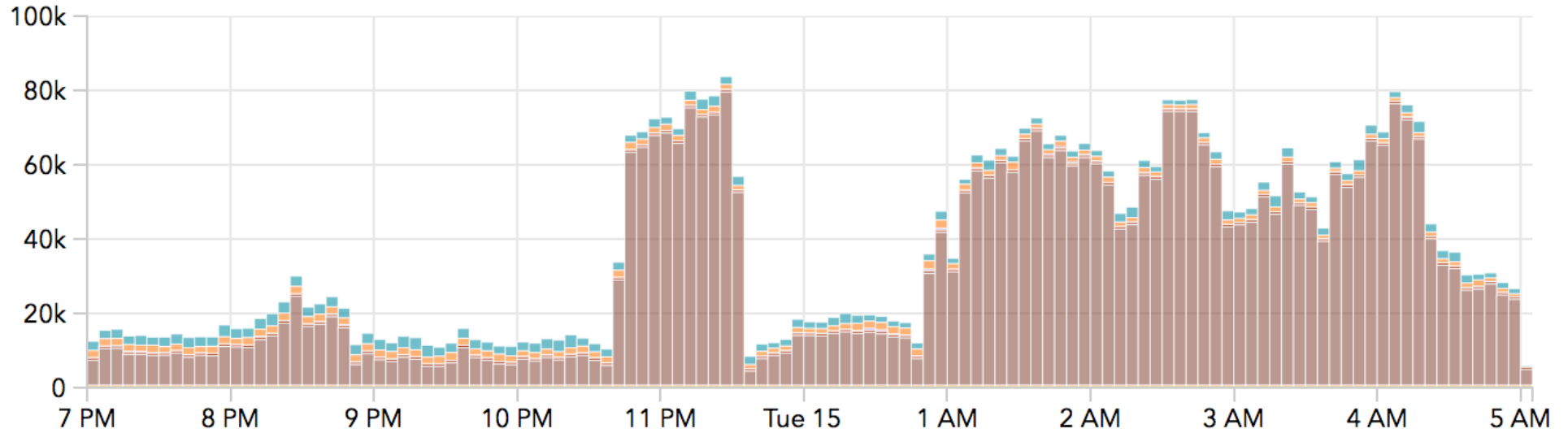


SQL Injection	7.94k
Cross Site Scripting	5.54k
Command Execution	1.02k
Directory Traversal	1.57k
Attack Tooling	13
Backdoor	10

Time	Request	Flags	Source	HTTP Responses
Sep 16, 2015 05:08:12 UTC	GET [REDACTED] [REDACTED]fs View request detail.	<b>SQLI</b> guests=%' AND 9481=DBMS_PIPE.RECEIVE_MESSAGE(CHR(80)  CHR(102)  CHR(75)  CHR(76),5) AND '%'='  <b>Attack Tooling</b> sqlmap/1.0-dev (http://sqlmap.org)	182.253.[REDACTED] [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.	<b>SQLI</b> guests=' AND 9481=DBMS_PIPE.RECEIVE_MESSAGE(CHR(80)  CHR(102)  CHR(75)  CHR(76),5) AND 'lhYf'='lhYf	182.253.[REDACTED] [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'





● 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

Security is  
Empowered







**Developers are  
interested in security**

- ~~Write code meant to be read~~  
Write code meant to be read *in a diff*
- Filtered out the dumb stuff before deploy
- Deploy small chunks, regularly
- Make Security Visible
- Watch what happens



The easier cooking seems, the more  
it needs to be watched, as the margin  
of error is bound to increase.

Fulvio Pierangelini

Nick Galbreath  
nickg@signalsciences.com  
@ngalbreath

goto;  
conference



*Please*

**Remember to  
rate this session**

*Thank you!*



Nick Galbreath  
nickg@signalsciences.com  
@ngalbreath

goto;  
conference

# Thanks !