AN UNLIKELY ROMANCE

THE CURRENT STATE OF BUG BOUNTIES

bugcrowd

YOUR SPEAKER

FOUNDER & CEO
PEN TESTER
HACKER
FATHER

WIDE ADOPTION OF CROWDSOURCED SECURITY

Financial Services

DISCOVER

MasterCard

WESTERN UNION

Consumer Tech

Pinterest

Spotify

fitbit

Retail & Ecommerce

jet

indeed
one search. all jobs.

lyst

Infrastructure Technology

Barracuda

twilio

aruba
NETWORKS

heroku

Automotive

FCA
FIAT CHRYSLER AUTOMOBILES

TESLA

Security Technology

1Password

okta

LastPass

Other

OWASP

(ISC)²

ZEPHYR
HEALTH

WHAT IS A BUG BOUNTY?

Independent security researchers from all over the world are recruited

Vulnerabilities are found and reported

Rewards are exchanged for reporting vulnerabilities in company applications

112
Countries

50K+
Researchers

$5M+
Paid out

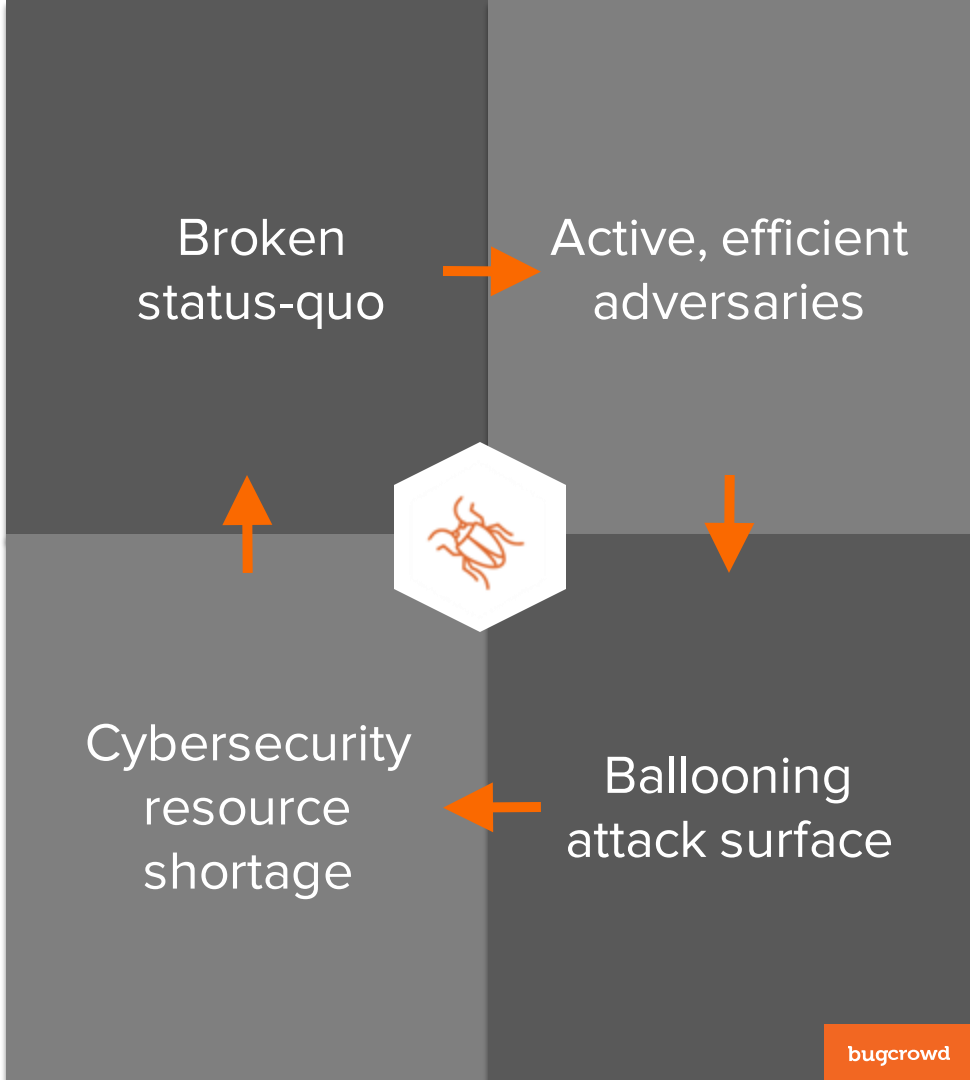
450+
Programs

85K
Submissions

110
Employees

WHY IS THERE AN ISSUE TO ADDRESS?

Breaking The Vulnerability Cycle



BROKEN STATUS QUO

$7.8B

Estimated Security Assessment Market Size by 2021

Source: http://cybersecurityventures.com/cybersecurity-market-report/

BALLOONING ATTACK SURFACE

1.1B

Websites as of January 2016...

...and the rest.

Source: http://www.internetlivestats.com/total-number-of-websites/

CYBERSECURITY RESOURCE SHORTAGE

209K

Unfilled cybersecurity jobs as of 2015

Source: http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth/

ACTIVE AND EFFICIENT ADVERSARIES

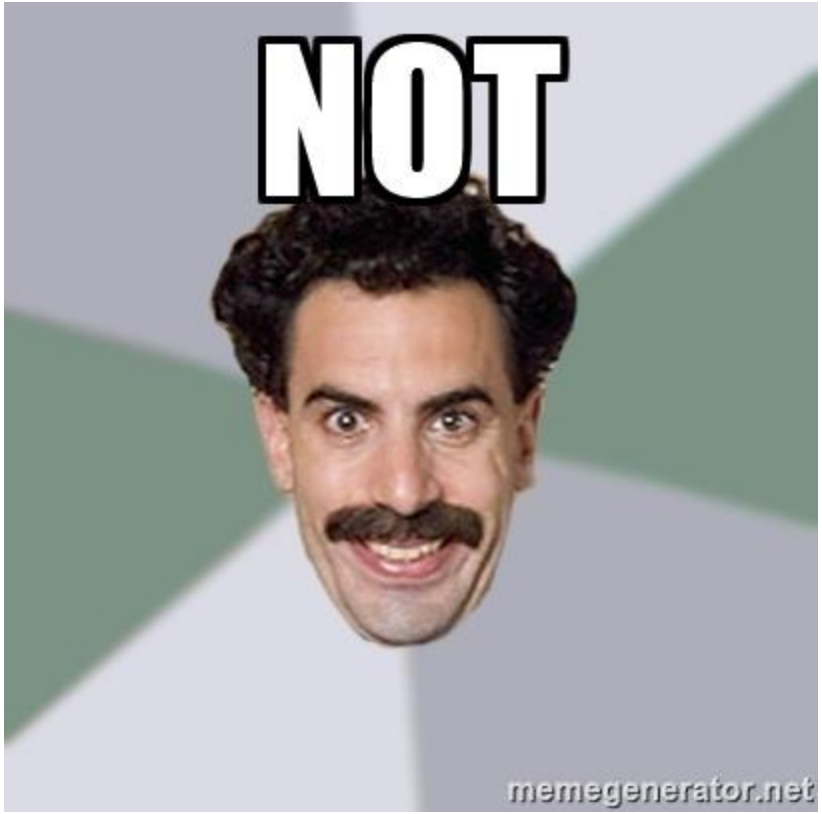
350%

Increase of breaches caused by hacking from 2007 to 2015

Source: http://www.idtheftcenter.org/2016databreaches.html

A SIMPLE SOLUTION...


AND
THEY LIVED
Happily
Ever After


NOT
memegenerator.net

WHAT ARE YOU WAITING FOR?

OBJECTIONS

If the model makes sense, what is stopping you?

Only crazy tech companies run bug bounty programs

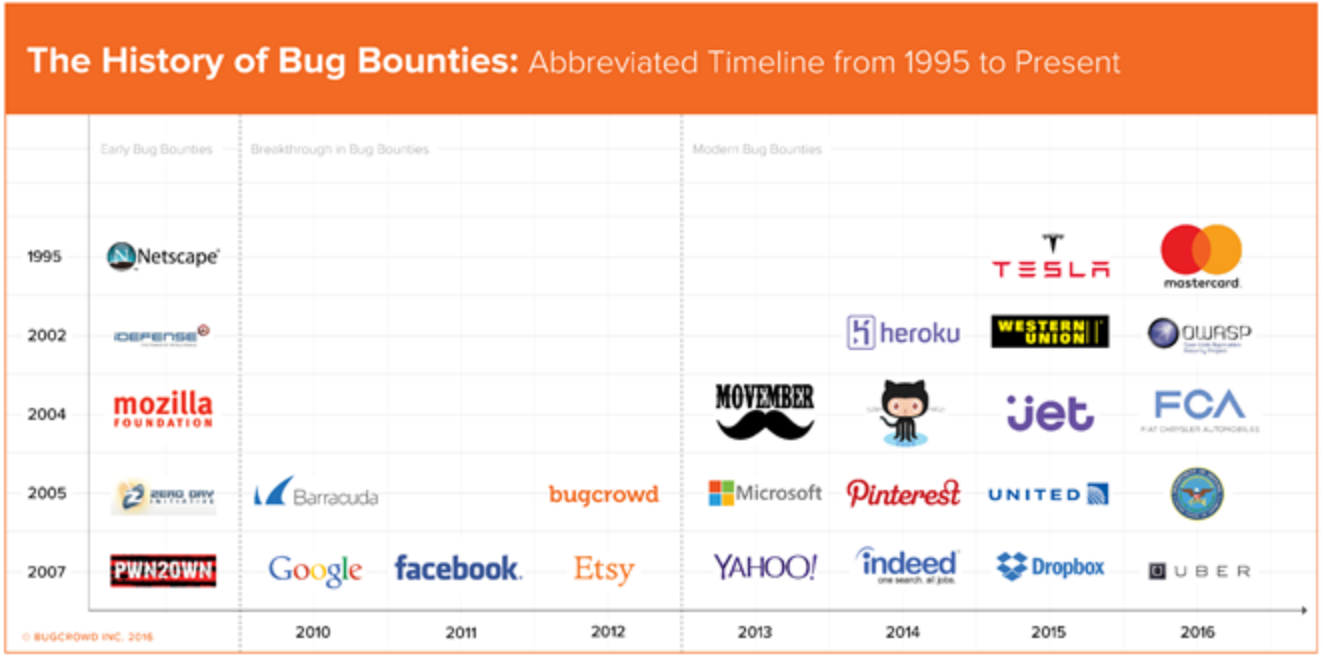
Bug bounties don't attract talented testers or results

They're too hard to manage and too expensive

Running a bounty program is too risky

IT'S WORTH IT.

OBJECTION: “ONLY TECH COMPANIES RUN BUG BOUNTY PROGRAMS”



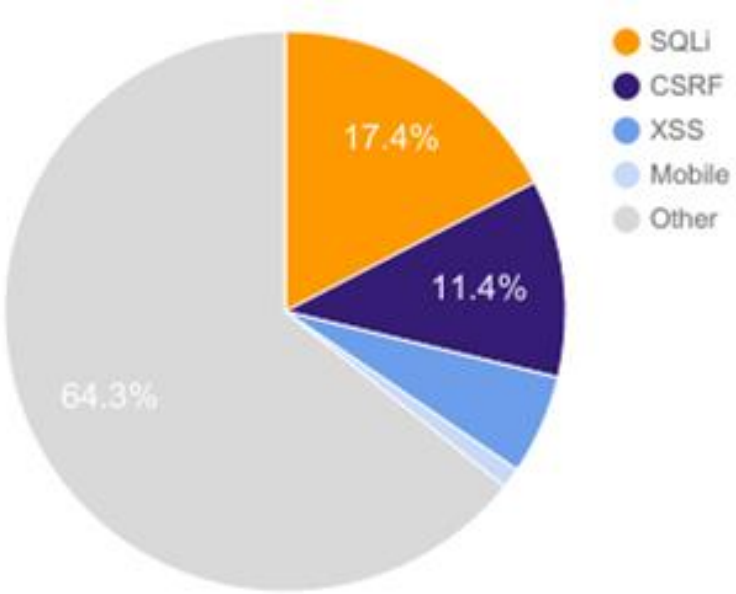
30%

of all bug bounty programs are run by Traditional organizations.

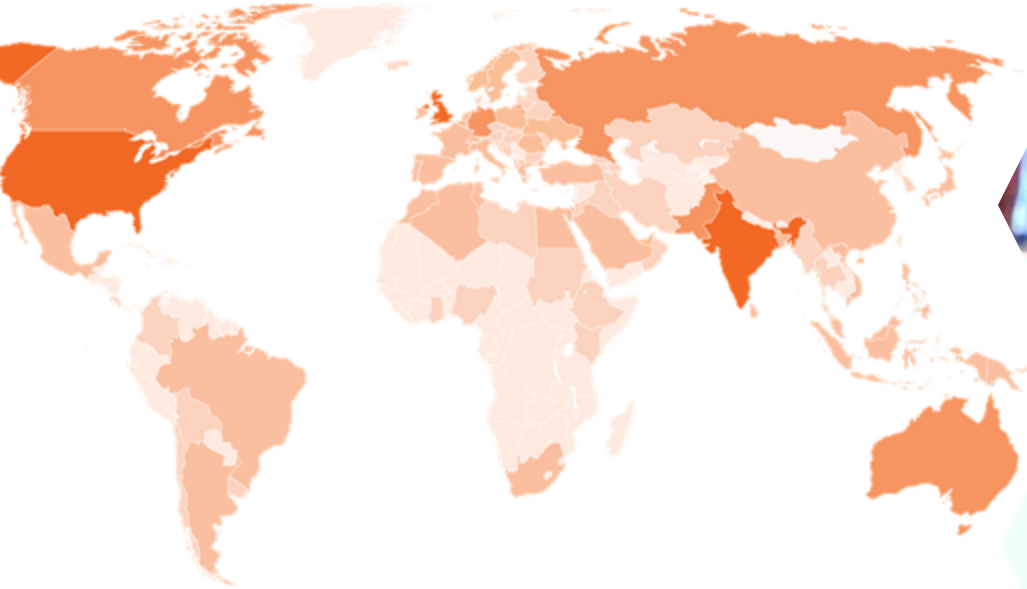
OBJECTION: “THEY DON’T ATTRACT TALENTED TESTERS OR RESULTS”

In 2016, a critical issue was reported every...

13 HRS



OBJECTION: “THEY DON’T ATTRACT TALENTED TESTERS OR RESULTS”



VIRTUOSOS

PROTECTORS

KNOWLEDGE SEEKERS

HOBBYISTS

FULL-TIMERS

"We decided to run a bug bounty program **to get access to a wide variety of security testers**. Hiring security researchers is very difficult in today's market..."

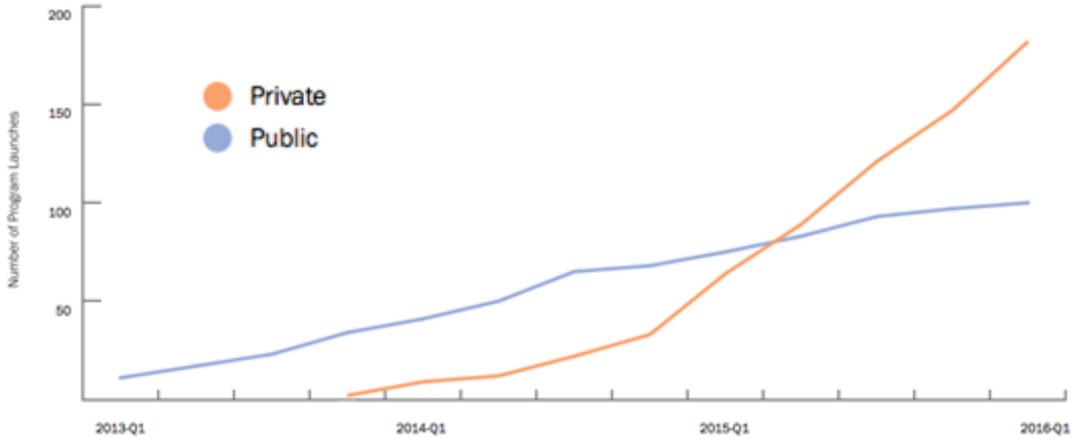
Jon Green
Sr. Director of Security Architecture

aruba
a Hewlett Packard Enterprise company

OBJECTION: “THEY’RE TOO HARD TO MANAGE AND TOO EXPENSIVE”

68%

Of all bug bounty programs are private, or invite-only.



OBJECTION: “THEY’RE TOO HARD TO MANAGE AND TOO EXPENSIVE” (cont.)

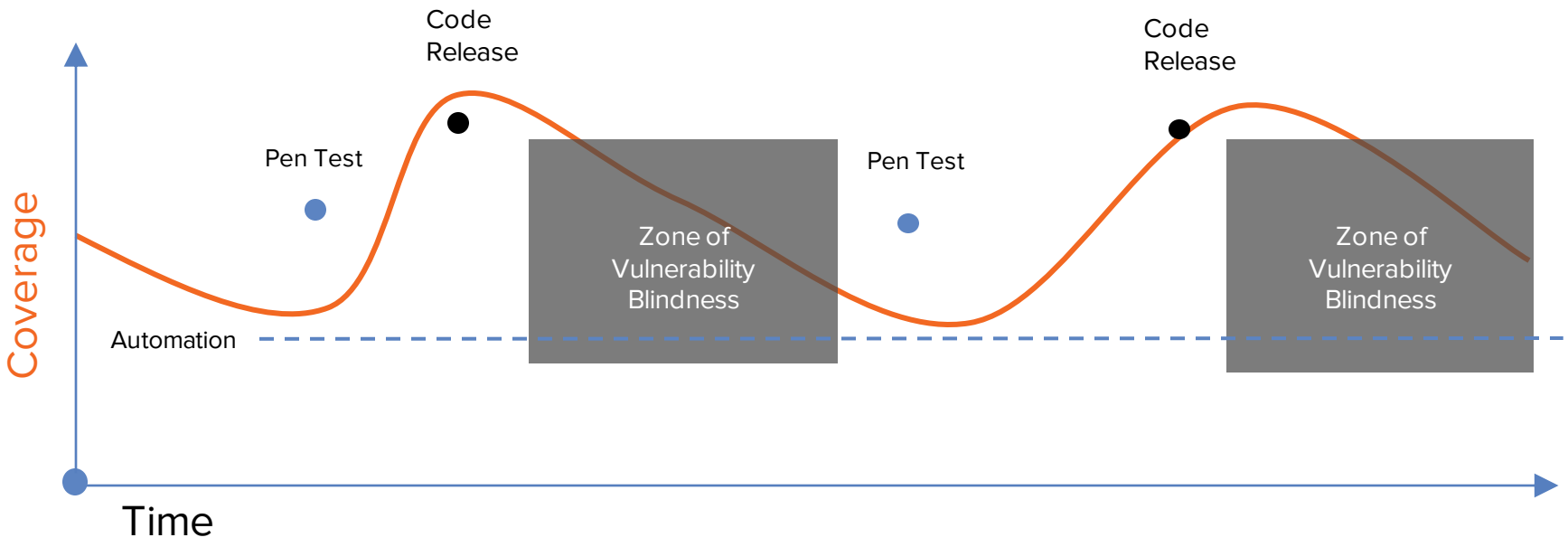
okta

David Baker
CSO

okta

Efficiency and effectiveness of the crowd is really why we bring them on... it's helped in expanding our team for a fraction of the cost. Now my internal resources are better utilized.

OBJECTION: “RUNNING A BOUNTY PROGRAM IS TOO RISKY”



In reality, public disclosure incidents occur less than

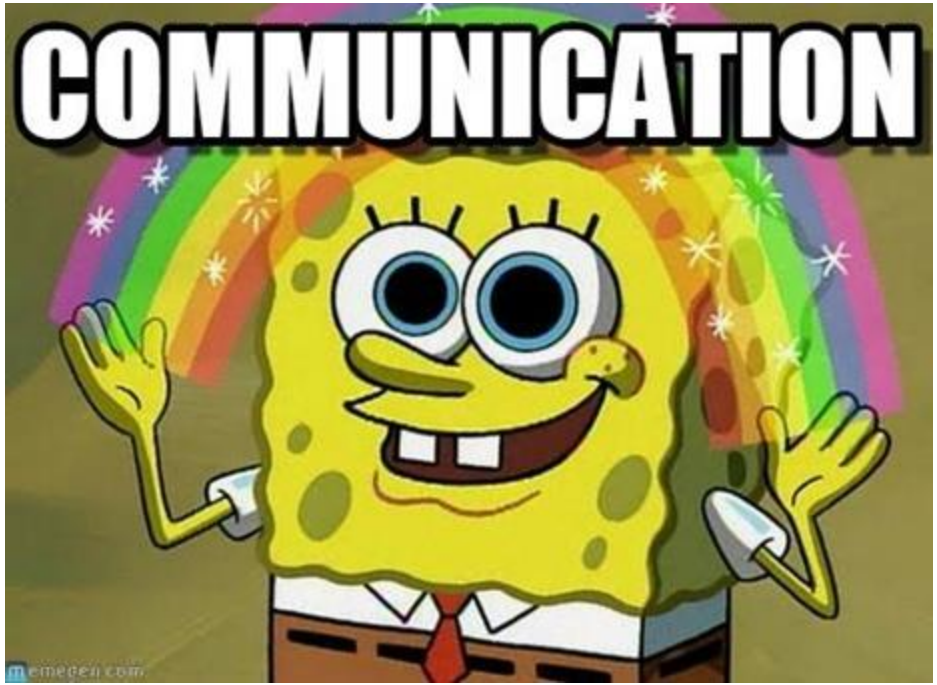
.0005%

of the time

HOW TO HAVE A HEALTHY RELATIONSHIP...

ALIGN EXPECTATIONS

COMMUNICATE OPENLY



PAY FAST, PAY WELL

QUESTIONS?

In 2016, a critical issue was reported every...

13 HRS

BROKEN STATUS QUO (cont.)