RSAConference2018
San Francisco | April 16–20 | Moscone Center

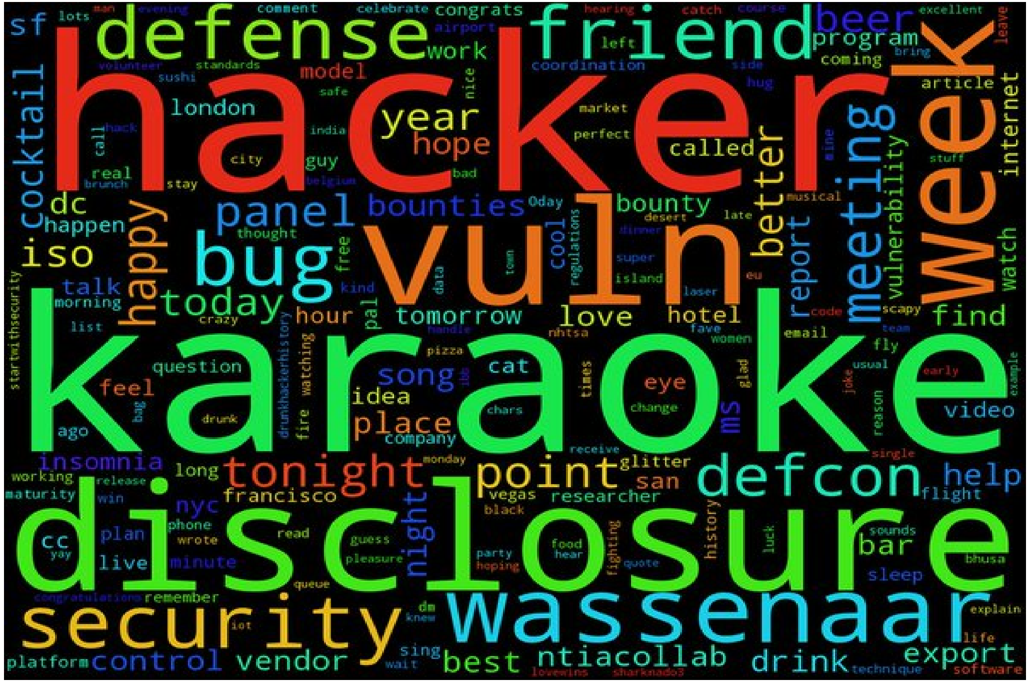
SESSION ID: EXP-R02

BUG BOUNTY BUZZWORD BINGO – DEEP DIVE UNDER A JUMPED SHARK

Katie Moussouris

Founder and CEO
Luta Security
@k8em0 (that's a zero, pronounced Katie Mo, not Kate Emo!)
@LutaSecurity (pronounced "LOOT-uh" with a hard "t")

What is it that you do here?



- Founder & CEO **Luta Security**
- Former **Microsoft** Security Strategist
- Former **Hacker** for Hire
- **ISO Standards** Editor
- **New America** Cyber Fellow
- **MIT Sloan** Visiting Scholar
- **Harvard Belfer** Affiliate
- **Cyber Export Control** Re-Negotiator

Advisor to Regulators, Lawmakers, Military & Government

Testifying before US Senate on Uber Data Breach Bounty Coverup And Making T-Rex Arms on CSPAN[1]

The picture I send to my family to explain my job

PREPARE YOUR BUZZWORD BINGO CARDS

…And Prepare to Free Your Mind

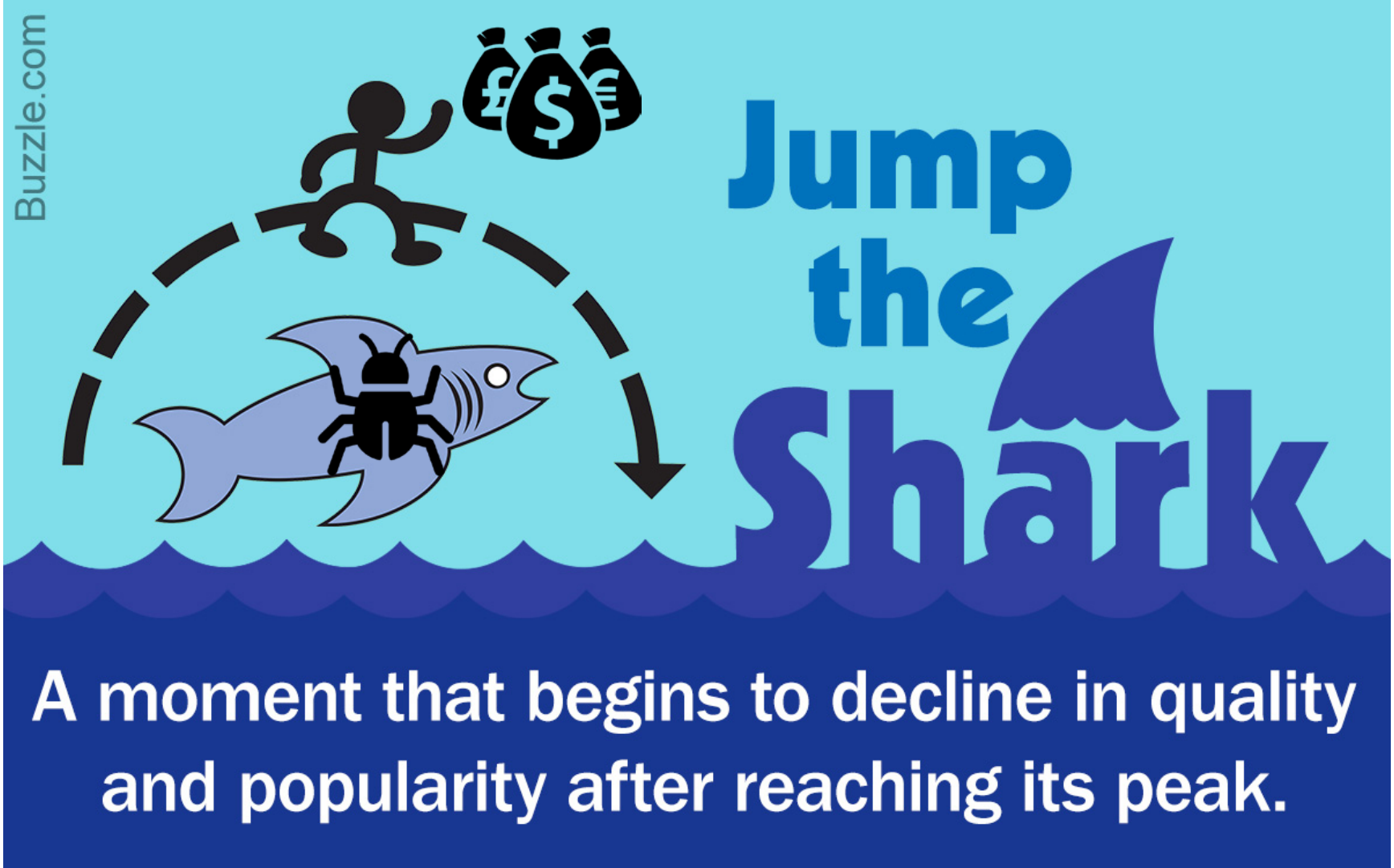
Wait…Sharks Don't Even Eat Bugs…Do They?!

Ehhhhhhhhhhh…..

Rather than ask your elders:

JUMPING THE SHARK = THE MOMENT WHEN A BRAND, DESIGN, OR CREATIVE EFFORT'S EVOLUTION LOSES THE ESSENTIAL QUALITIES THAT INITIALLY DEFINED ITS SUCCESS AND DECLINES, ULTIMATELY, INTO IRRELEVANCE

Wikipedia, 2013


Buzzle.com
Jump the Shark
A moment that begins to decline in quality and popularity after reaching its peak.

HOW DID WE END UP ALL THE WAY OUT HERE?

Who Knew This Would Become a THING?

Your Lips Are Moving But There's No Sound

The Cyber Security Opportunity

Cyber Security is the Fastest Growing Tech Sector Worldwide

The worldwide cyber security market will reach $170 Billion by 2020; Overall security market will grow at a 7.8 % CAGR through 2019*

$655 Billion will be spent on cyber security initiatives to protect PCs, mobile devices, and IoT devices through 2020.**

Government spending on cybersecurity has increased at an average annual rate of 14.5% between FY 2006 and FY 2017, outpacing procurement in every other type of major government program.***

Cloud security market to be worth $12 billion by 2022****

The Healthcare Cyber Security Market will hit $10.85 Billion By 2022***

The U.S. financial institutions cybersecurity market is the largest and fastest growing private sector cyber security market; cumulative 2016-2020 size is forecasted to exceed $68 Billion****

*Gartner: Forecast Analysis: Information Security, Worldwide, 4Q15 Update
** Markets and Markets: "Cyber Security Market by Solutions"
***Jones, Lang, Lasalle, IP
**** Transparency Market Research: Cloud Security Market - Global Industry Analysis, Size, Share, Growth, Trends and Forecast 2014-2022
*****Grandview Research: Healthcare Cyber Security Market Size, Analysis Report, 2022
******U.S. Financial Services: U.S. Financial Services: Cybersecurity Systems & Services Market – 2016-2020"

GDPR increases costs in both compliance & fines

Cost of Data Breaches Predicted to top 2 TRILLION USD by 2019

LUNA SECURITY

And Yet, Here We Are

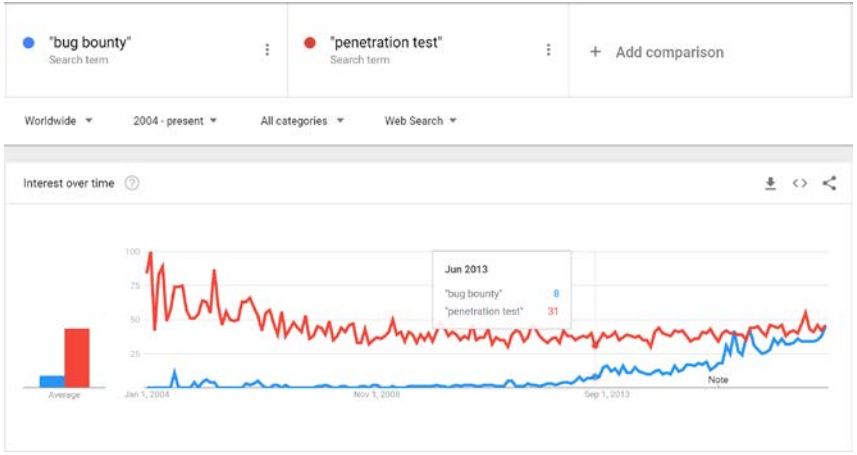
Even When A Patch Is Available We Are Still Practicing Security Theatre

Increased Security Spending ≠ Increased Security

Google Knew. Google Always Knew (since 2004)

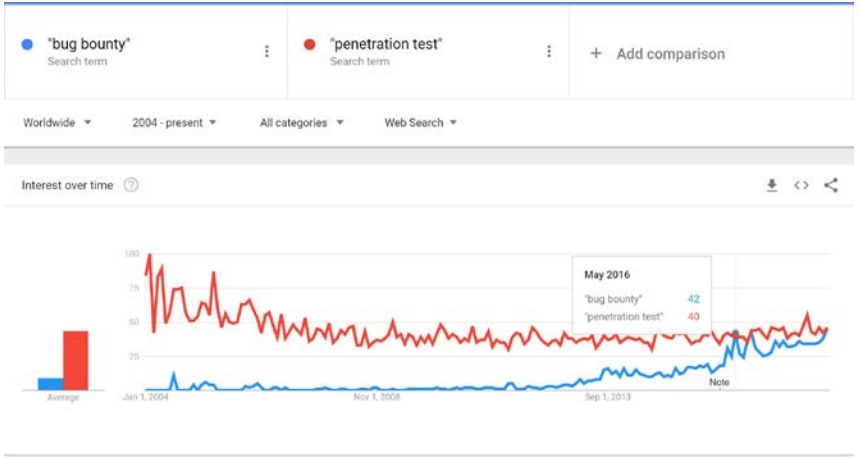
Inflection Point #1:

Fitting Earths into Jupiter's Storm

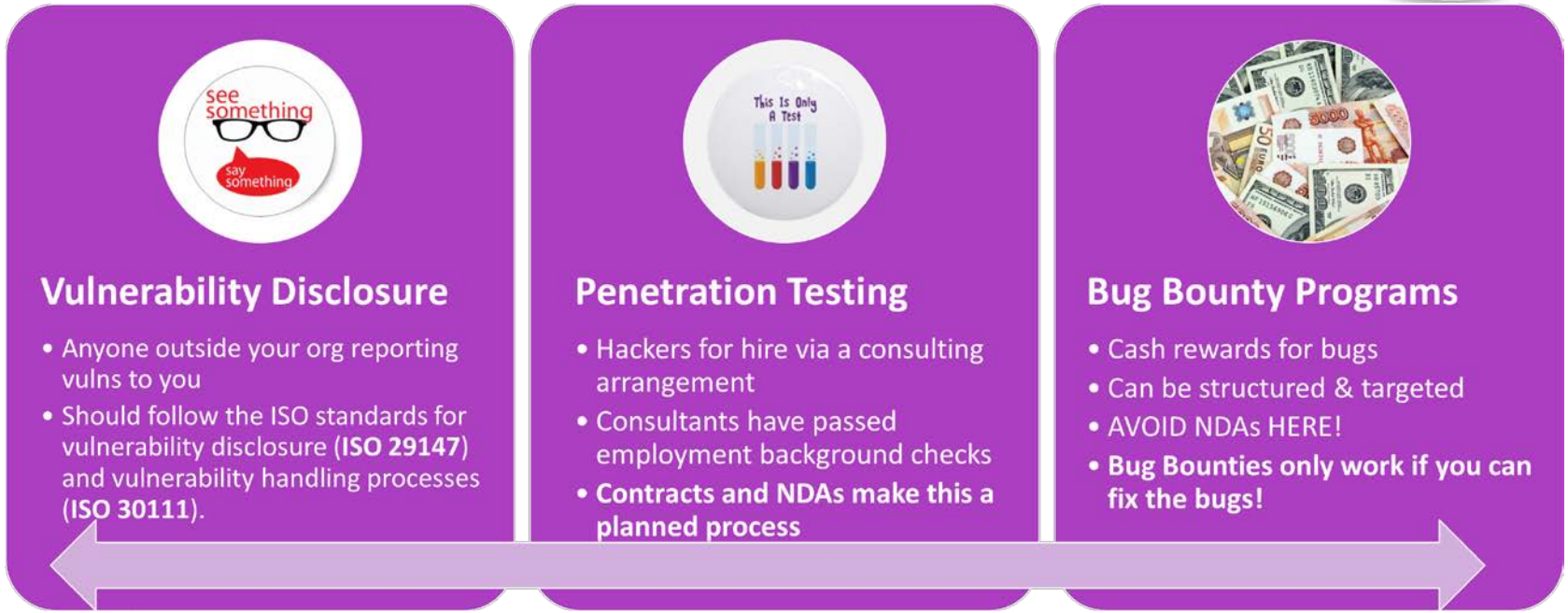


Inflection Point #2:

5 Sides to Every Story



Vulnerability Disclosure vs. Pen Test VS. Bug Bounty



94% of the Forbes Global 2000 have NO PUBLISHED WAY to report a security vulnerability.

EASY!! LET'S JUST OPEN THE FRONT DOOR

…We Take Security Very, Very Seriously! We Now Pay a Bug Bounty!! What could possibly go wrong?!

Was This What You Were Expecting?

How About This?

- How Do We Distinguish Friend From Foe?
- What About Data Privacy?
- Do NDAs Protect My Organization?
- Do NDAs shield helpful hackers from Legal Harm?

And This?? What About This?

If You Cannot Handle Incoming Bug Reports from Today's Sources, What Hope Do You Have Against more Autonomous Vulnerability Discovery Methods?

Isn't This Problem Solved By Bug Bounty Platforms?

Manage the Flood, They Said

Only Validated Bugs, They Said

Totally Not Relying on God-like Superpowers & Endless Skilled Triage Labor

Triage Labor – The Job You'll Never Love

Microsoft receives between 150,000-200,000 non-spam email messages per year to secure@Microsoft .

In 2007, Popular Science named "**Microsoft Security Grunt**" among the **Top 10 Worst Jobs in Science**.

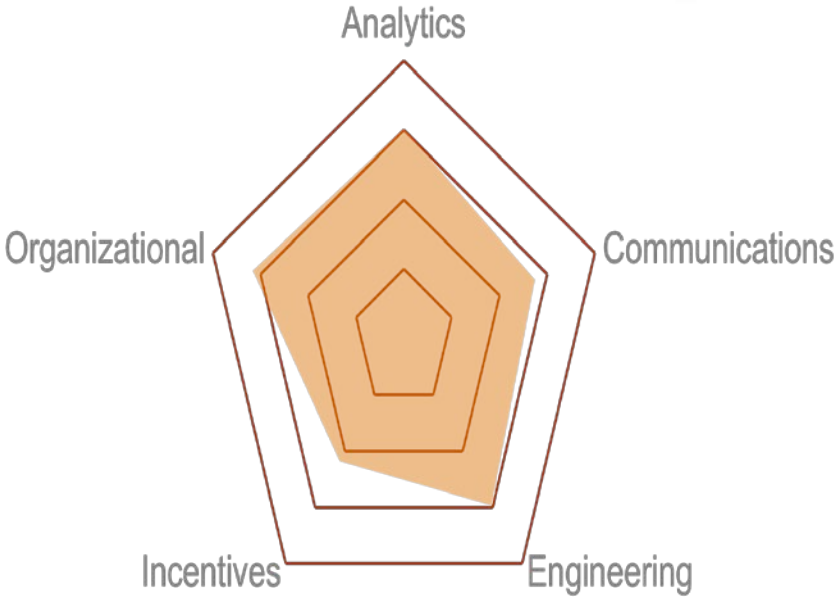
- This lands the triage/case management job between "**Whale Feces Researcher**" and "**Elephant Vasectomist**"
- This role is full-time, **pays six figures plus full benefits**, is held by several team members, & has the **highest turnover** of any job in the Microsoft Security Response Center

Capacity Planning & Maturity is the Right Way Forward

Turns Out, There IS Such a Thing as Too Much Chocolate!

Vulnerability Coordination Maturity Model

- Model guides how to organize and **improve vulnerability coordination** processes
- **5 Capability Areas**: Organizational, Engineering, Communications, Analytics and Incentives[2]
- **3 Maturity Levels** for each Capability: Basic, Advanced or Expert
- Organizations can **benchmark** their capabilities
- Creates a **roadmap** for success



Paying for Bugs vs Actually Becoming More Secure

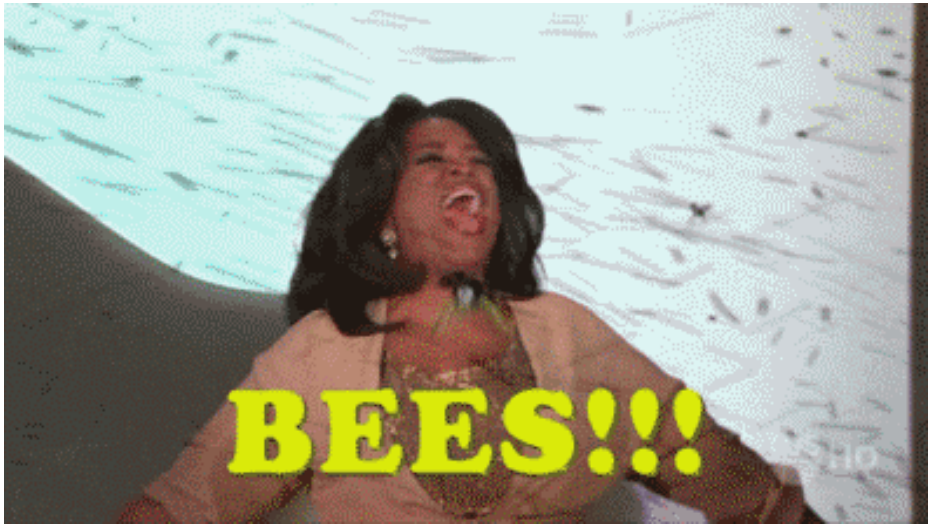
- Majority of bug bounty bugs are XSS
- Breaches often caused by low-hanging fruit (e.g. insecure S3 buckets)
- Trendy bug bounties replacing basic security self-care
- One cannot pen-test or bounty one's way to security

#NotAllBugs Are Created (or Fixed) Equally

Creating a Vulnerability Typology

Vulnerability Characteristics	Quantity of Vulnerabilities	➢	Scarce - Numerous
	Ease of Vulnerability Discovery	➢	Easy - Difficult to Find
	Likelihood of Vulnerability Rediscovery	➢	Low - High
Patching Dynamics	Technical Difficulty of Remediation	➢	Easy - Hard to Fix
	Logistical Difficulty of Remediation	➢	Easy - Hard to Access
	Average Life of a Vulnerability	➢	Short - Long
Market Dynamics	Third Party Market for Vulnerability	➢	Offensive, Defensive, Mixed, Etc.
	Market Size	➢	Small - Large
	Bug Bounty Program	➢	Yes, No
Human Dynamics	Attackers	➢	Criminals, States, Patriots, Etc.
	Researcher Pool	➢	Small - Large
	Attacker Motivation	➢	Political, Financial, Reputational

Do You Want Ants? Because This is How You Get Ants

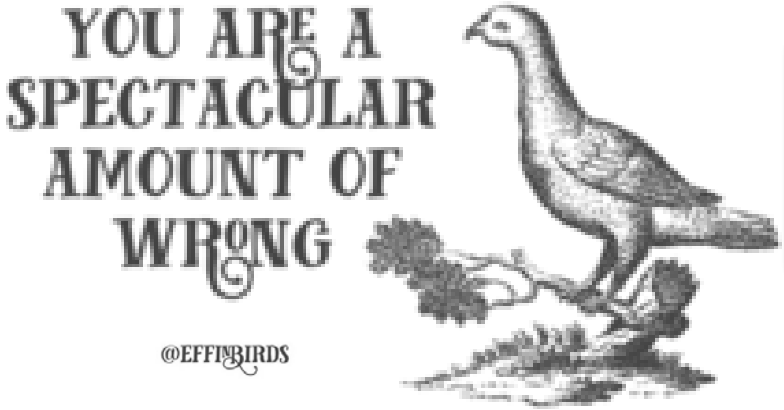


These Aren’t the Bugs You’re Looking for. Move Along.

OF MYTHS, MOTIVATIONS, AND MARKETS

…or Raise Your Hand If You've Never Broken Any Laws

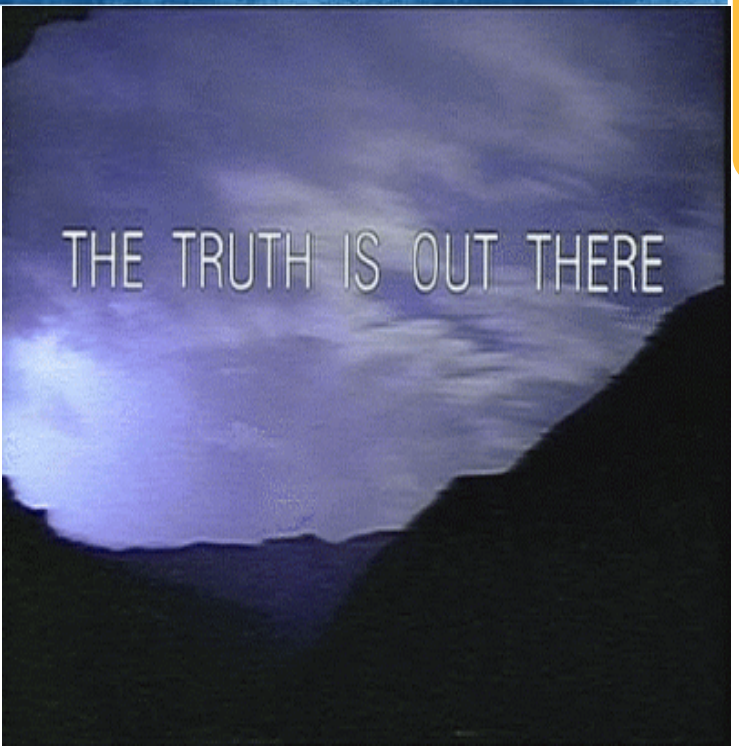
Bug Bounty Myths Defy Behavioral Economics



MYTH: Bug Bounties are the logical end goal of all vulnerability disclosure programs

MYTH: Hackers will only look for bugs in exchange for **cash**

MYTH: You have to **outbid the offense market**



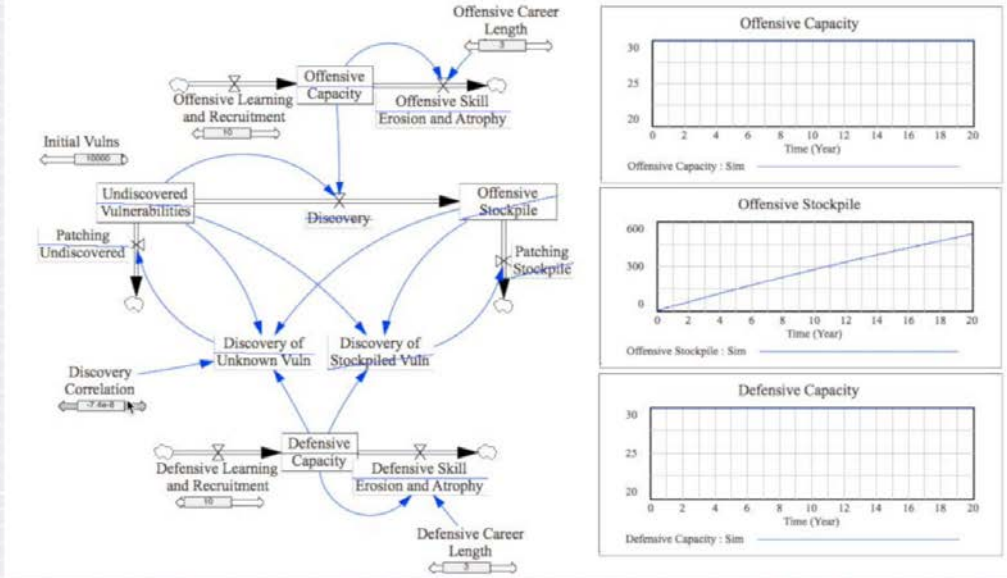
TRUTH: Bug Bounties are not a replacement for penetration testing, nor do they alone indicate security maturity

TRUTH: Hackers, like all humans, have a **mixed matrix of motivations**

TRUTH: The Defence Market for bugs can only go so high

There is More To This Than Money

The 0day Market System Dynamics Model



From 2015 Research with MIT & Harvard on the System Dynamics of the 0Day market:

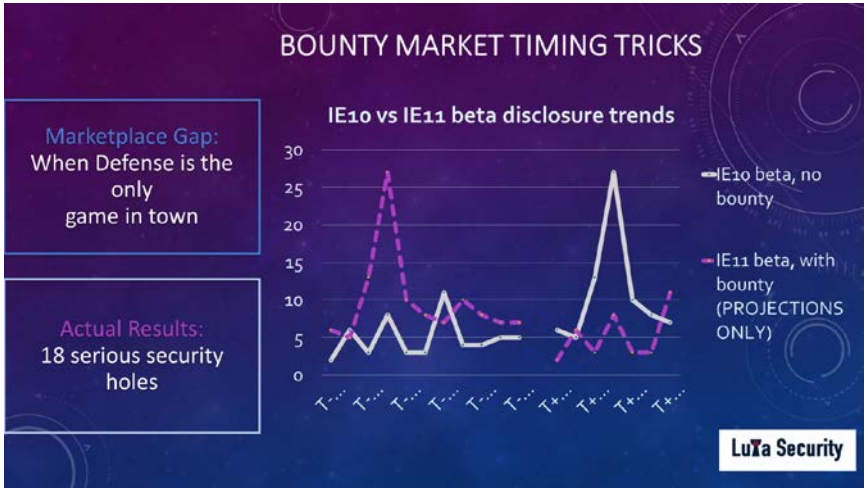
"The Wolves of Vuln Street"[3]

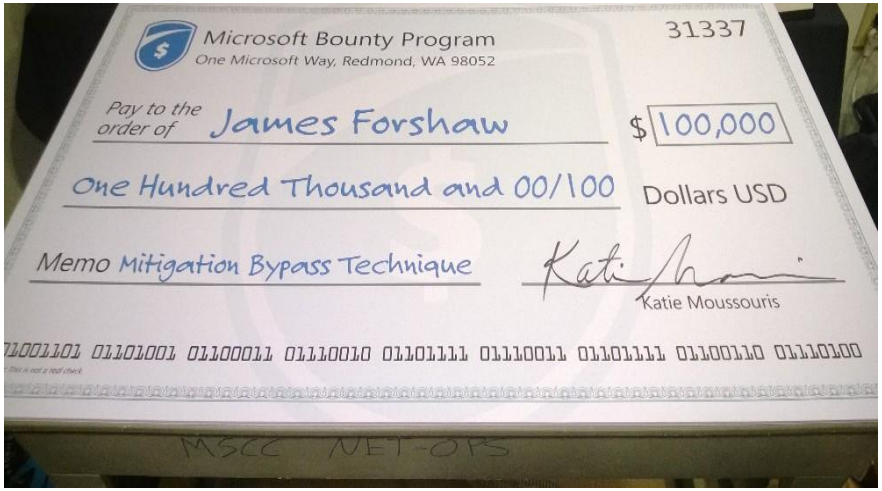
PERVERSE INCENTIVES

And Ways To Avoid Them

Perverse Incentives – Lessons from 1995

Know Your Bugs, Know Your Market, Know Your Audience





Bounty Smarter, Not Harder

Hack the Pentagon – Hack the Planet!

BY THE NUMBERS

Registered eligible participants **1,410**

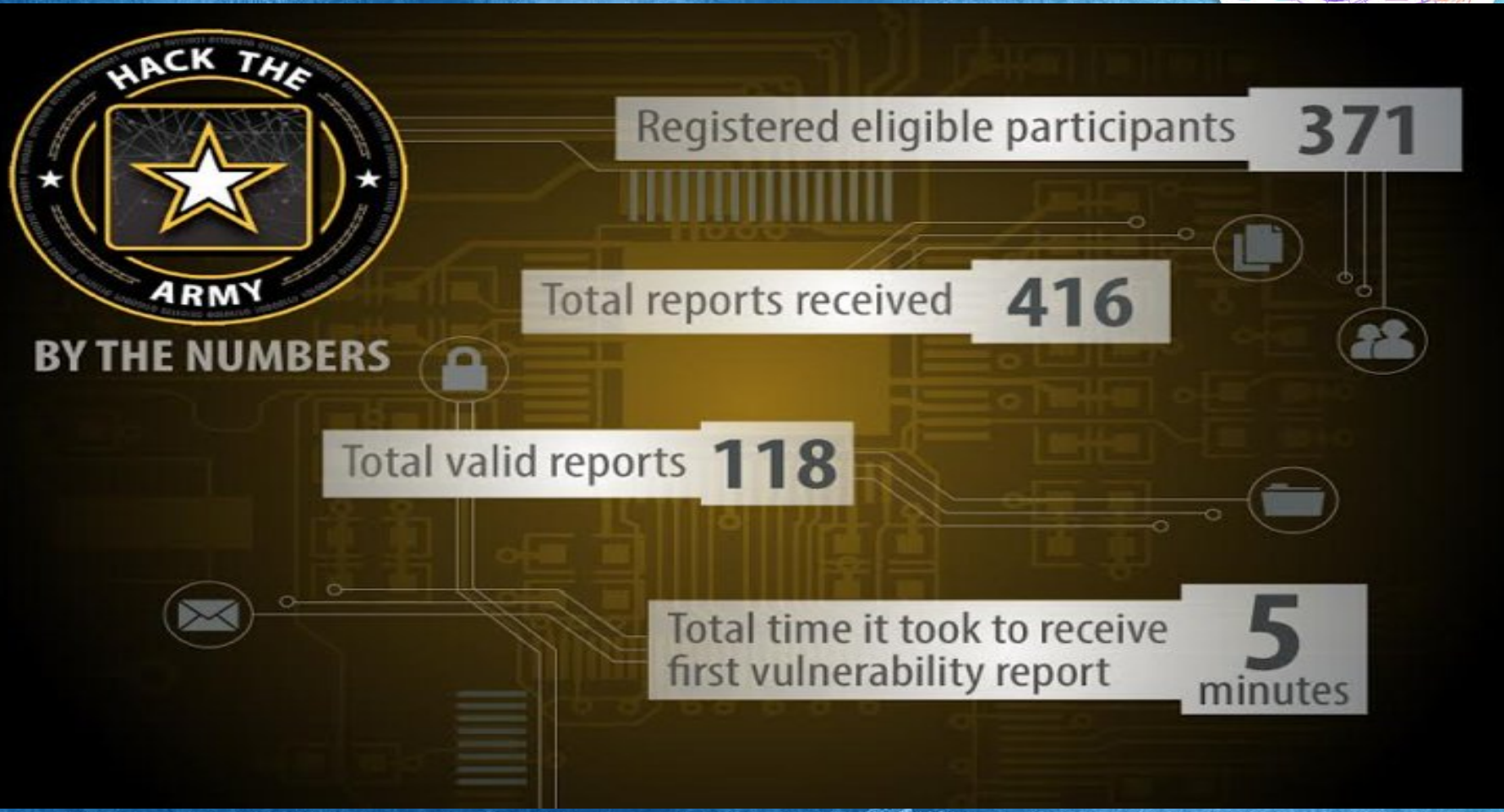
Total reports received **1,189**

Total valid reports **138**

Total time it took to receive first vulnerability report **13 minutes**

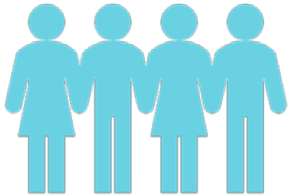
Hack the Army – Hack the Planet!

Hack The Army – Gently With a Chainsaw



Labor Market for Bug Hunting vs Bug Fixing & Code Writing

- The [bug hunting] labor market is **highly-stratified**…characterized by a minority of…lucrative workers and a majority of low-volume…low-earning workers"[3]
- Tiny fraction of talent; Majority generate **noise**
- Bug bounty hunting celebrated for outpacing median developer salaries (16x in India)?!
- Top 10 CS programs in US universities don't require security to graduate. 3/10 lack security electives.



MARKETS FOR BUGS & LABOR ARE BEING SHAPED…

And It's Coming From Inside the House! And the Senate!

Hack the DHS! Hack the State Department!

What I Say

"There's an **absolute misunderstanding** by members of Congress who say 'let's just repeat the success of Hack the Pentagon,'" Moussouris said.

"all the work that went into making Hack the Pentagon successful is that now **people think it's easy and it's not**."

What Pentagon Insiders Say

"The Defense Department has an **enormous workforce that's responsible for [patching]"** said Lisa Wiswell, a former top Defense Department cyber adviser **who helped organize the Pentagon bug bounty**

"Forgive the example, but who the hell's at the **Department of the Interior to fix their stuff**?" Wiswell asked.

I Know! Let's Just Pass a Law that Says "Be Secure!"

What Bug Bounty Platforms Say

"the HackerOne CEO, similarly acknowledged that some civilian agencies **may not be mature enough for bug bounties**, but said he **nevertheless supports the legislative push** for them."

"lawmakers know they have to set a bar and set a mandate for this and we should support that…**I don't think any action is happening too fast**."

AHA!! YOU'RE A BUG BOUNTY APOSTATE!!

Bug Bounties Are Good For

Finding bugs you missed after you perform your own security development & deployment processes

Recruiting!

Focusing eyes on your work via timing or via hard problem solving

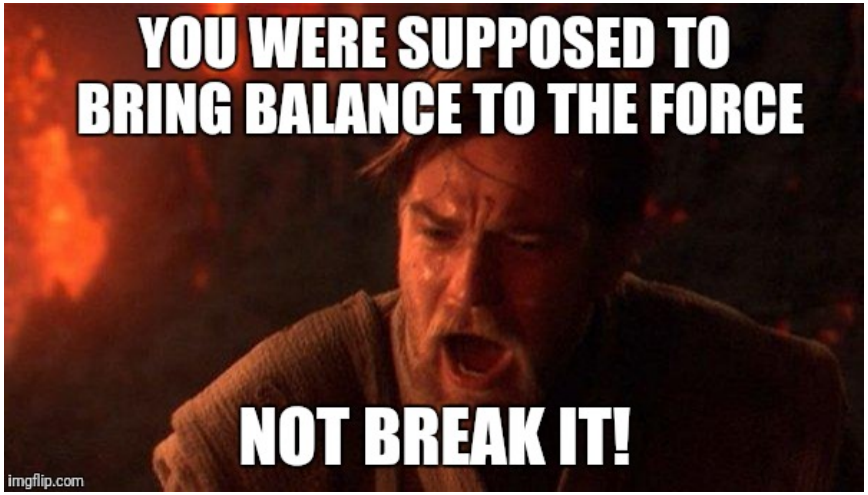
Bug Bounties Are Bad For

Your First External Bug Reports (unless you are teeny tiny!)

Employee morale if you consistently pay more to outsiders without alleviating internal resource pressures

Data privacy, unless you've really spent time thinking through & planning for in-scope & out-of-scope scenarios

In All Things, BALANCE



Creation, Maintenance, Destruction

Meditate on the Wabi Sabi World Wide Web – And Take Action

This Month:	**Audit your own systems & software**	**E**liminate low-hanging fruit
Next 2 Quarters:	**Build a** sustainable vulnerability handling process	**Learn** from each bug to e**liminate entire classes of vulnerabilities**
Within 1 Year:	Bring **balance** to the labor workforce	Hire/outsource intelligently
ALWAYS:	Beware of **perverse incentives**	Question Anything Too Good to Be True

References.

Questions?

Thank You!

- [1]https://www.commerce.senate.gov/public/?a=Files.Serve&File_id=E162FD54-F858-44AE-B25F-64E331C628AE
- [2]Ryan Ellis, Keman Huang, Michael Siegel, **Katie Moussouris**, and James Houghton. “Fixing a Hole: The Labor Market for Bugs.” New Solutions for Cybersecurity. Howard Shrobe, David L. Shrier, and Alex Pentland, eds. Cambridge: MIT Press. In Press. ISBN: 9780262535373 https://mitpress.mit.edu/books/new-solutions-cybersecurity
- [3]https://www.rsaconference.com/writable/presentations/file_upload/ht-r04f-but_now_i_see_-_a_vulnerability_disclosure_maturity_model.pdf
- [4]https://www.rsaconference.com/writable/presentations/file_upload/ht-t08-the-wolves-of-vuln-street-the-1st-dynamic-systems-model-of-the-0day-market_final.pdf

- Katie at Lutasecurity dot com
- @LutaSecurity @k8em0

LUTA SECURITY