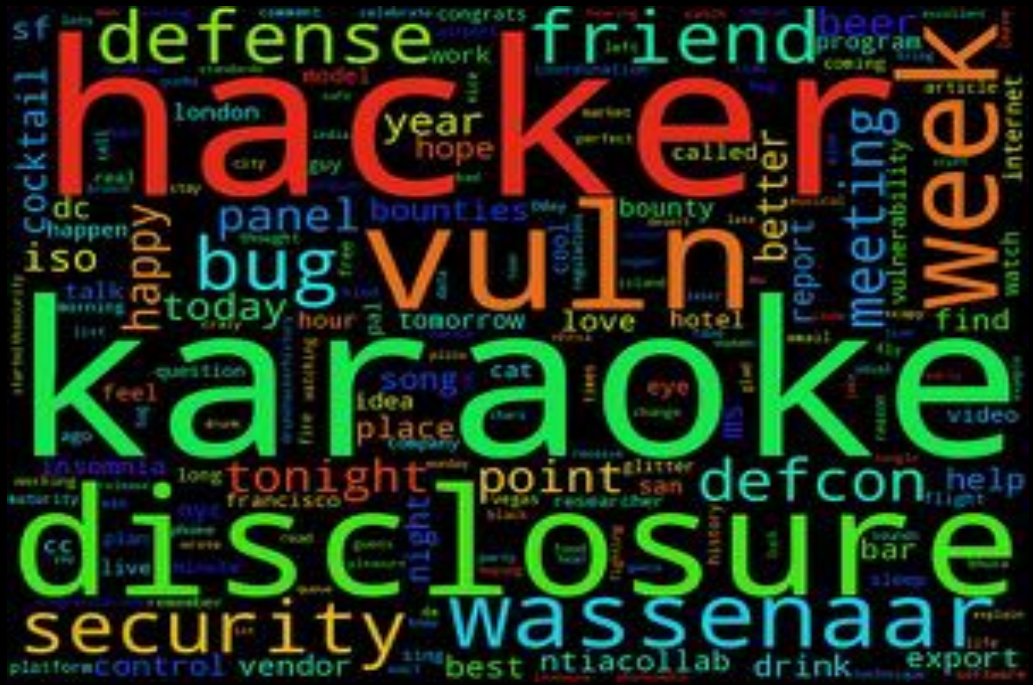
Security Should Be Smarter Not Harder

Katie Moussouris
Luta Security

Risk Management vs Trendy Topics

What is it that you do here?



- Founder & CEO **Luta Security**
- Creator of Microsoft Bug Bounties
- Advisor to the Pentagon, NCSC
- Former **Hacker** for Hire
- **ISO Standards** Editor
- **New America** Cyber Fellow
- **MIT Sloan** Visiting Scholar
- **Harvard Belfer** Affiliate
- **Cyber Export Control** Re-Negotiator

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

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


How Did we get here?
Can’t we just throw more money at this problem?
SURPRISE!! Money Alone can’t buy you security

MARKETING!!!!!!!!!!!!!!!!!!!!!!!!!!!!111!1security!!!!

And Yet, Here We Are

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

Increased Security Spending ≠ Increased Security

Silver bullets are for werewolves

Vulnerability Disclosure vs. Pen Test vs. Bug Bounty

Vulnerability Disclosure

- Anyone outside your org reporting vulns to you
- Should follow the ISO standards for vulnerability disclosure (**ISO 29147**) and vulnerability handling processes (**ISO 30111**).

Penetration Testing

- Hackers for hire via a consulting arrangement
- Consultants have passed employment background checks
- **Contracts and NDAs make this a planned process**

Bug Bounty Programs

- Cash rewards for bugs
- Can be structured & targeted
- AVOID NDAs HERE!
- **Bug Bounties only work if you can fix the bugs!**

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 vewwy vewwy seriously!
Let’s just start a bug bounty!
What could possibly go wrong?!!!111!!
Surprise!! Everything.

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?

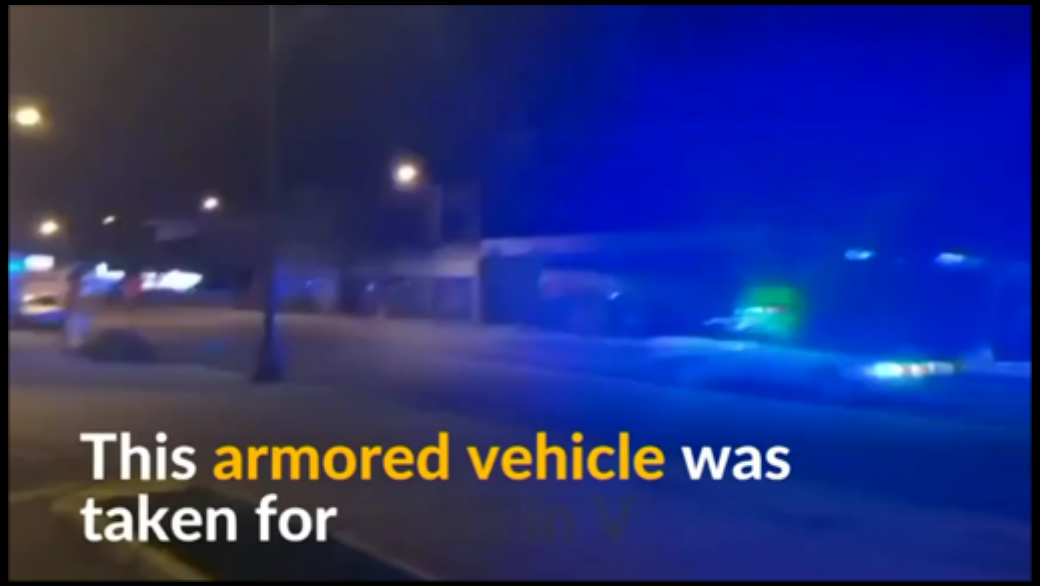
Welcome Our New Exploit Robot Overlords

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

Tank you for your service

Seriously though, take care of yourselves & each other.
https://veteranscrisisline.net 1-800-273-8255 TEXT to 838255

I had authorization!! I was running a test!!!



Real Incident Response Resources Spent Here
Instead of Other Security Response

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**.

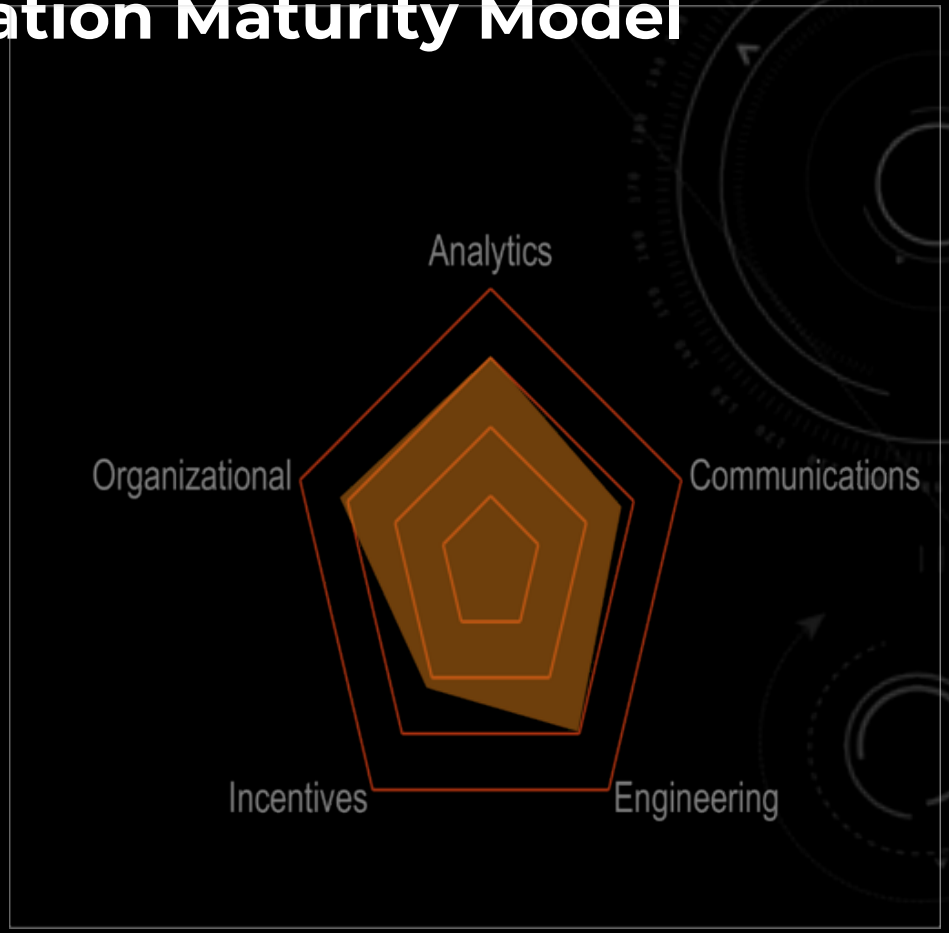
- This lands the triage/case management job between "**Whale Feces Researcher**" and "**Elephant Vasectomist**"
- This role is full-time, **pays six figures plus full benefits**, is held by several team members, & has the **highest turnover** of any job in the Microsoft Security Response Center

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



#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.

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 security due diligence
- One cannot pen-test or bounty one's way to security – THAT'S **BUG BOUNTY BOTOX!!!!!!**


Myths
Motivations
Markets
Or, raise your hand whoever hasn’t 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/"black" market**

Case In Point: Bug Bounty Botox

Katie Moussouris ✓
@k8em0

Incredibly great ROI for one top #bugbounty hunter.
Incredibly terrible ROI for the org paying this much for 4 hours of his professional time.
For those paying attention, he's one of about 100/350,000 on the platform who has made over $100k, 1 of 2 who cleared over $1M last year

dawgyg@Home @thedawgyg
The fist 6 figure pay day of 2019. $119,650 Thanks Oath and @Hacker0x01

8:11 AM - 12 Feb 2019

Katie Moussouris ✓
@k8em0

Replying to @k8em0 @S9k

Nobody's knowledge in security is worth $29k per hour that they could not have sourced more efficiently.
Project zero folks are among the most knowledgeable in security & exploitation in systems often hard to exploit & they don't make that.
He's not finding new classes of bugs.

8:26 AM - 12 Feb 2019

Why Would A Top Hacker Choose Less $$?!

Replying to @k8em0 @S9k

It was about 4 hours after finding the specific domain that I went after. It was an unknown domain to most so had not been picked through. Bug classes were only SQLi, SSRF and sensitive info disclosure

2 12

Katie Moussouris @k8em0 · Feb 12

Exactly. You certainly earned it. My point is different about org efficiency though. It's why Oath hired @BugBountyHQ . They should hire more like you folks. Grab the top 20 on the platform. Dream team.

1 2

scriptjunkie @scriptjunkie1 · Feb 12

Why would @thedawgyg accept that position getting paid far less than he currently makes?

3

Katie Moussouris @k8em0 · Feb 12

I'm not saying he would. @BugBountyHQ did, but he also gets to hunt other bounties on the side.

There are ways to make it work & everything is a trade-off. It might be all about $ now, but people's appetites for income uncertainty change over time. Everyone is different.

dawgyg@Home @thedawgyg · Feb 12

Replying to @scriptjunkie1 @k8em0 and 2 others

I actually was trying to join their team last year before the merge with Verizon etc. But it fell through the cracks during the moving around after their merge. I have actually been wanting/trying to work for Yahoo since the late 90s

1 3

scriptjunkie @scriptjunkie1 · Feb 12

Their loss!

2

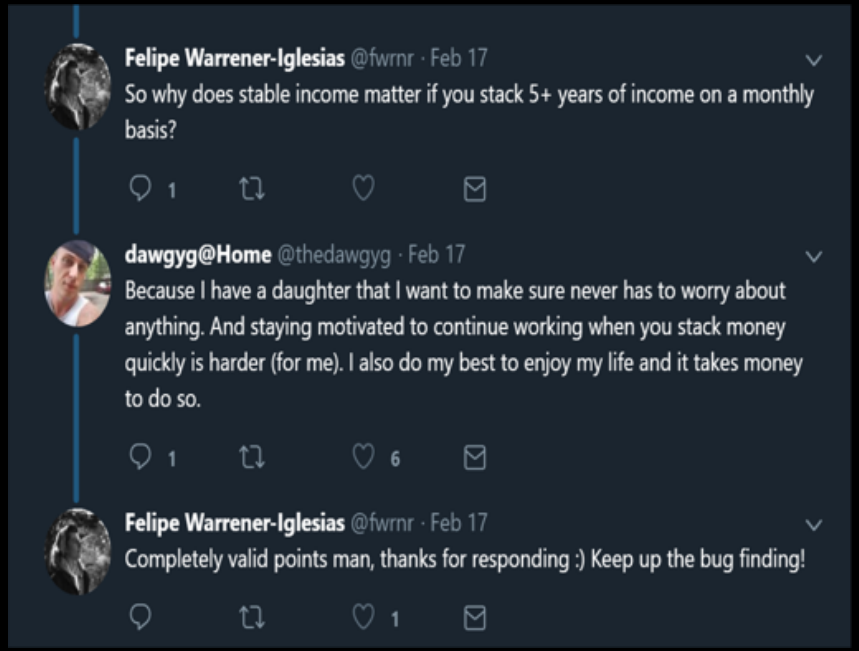
dawgyg@Home @thedawgyg · Feb 12

Replying to @scriptjunkie1 @k8em0 and 2 others

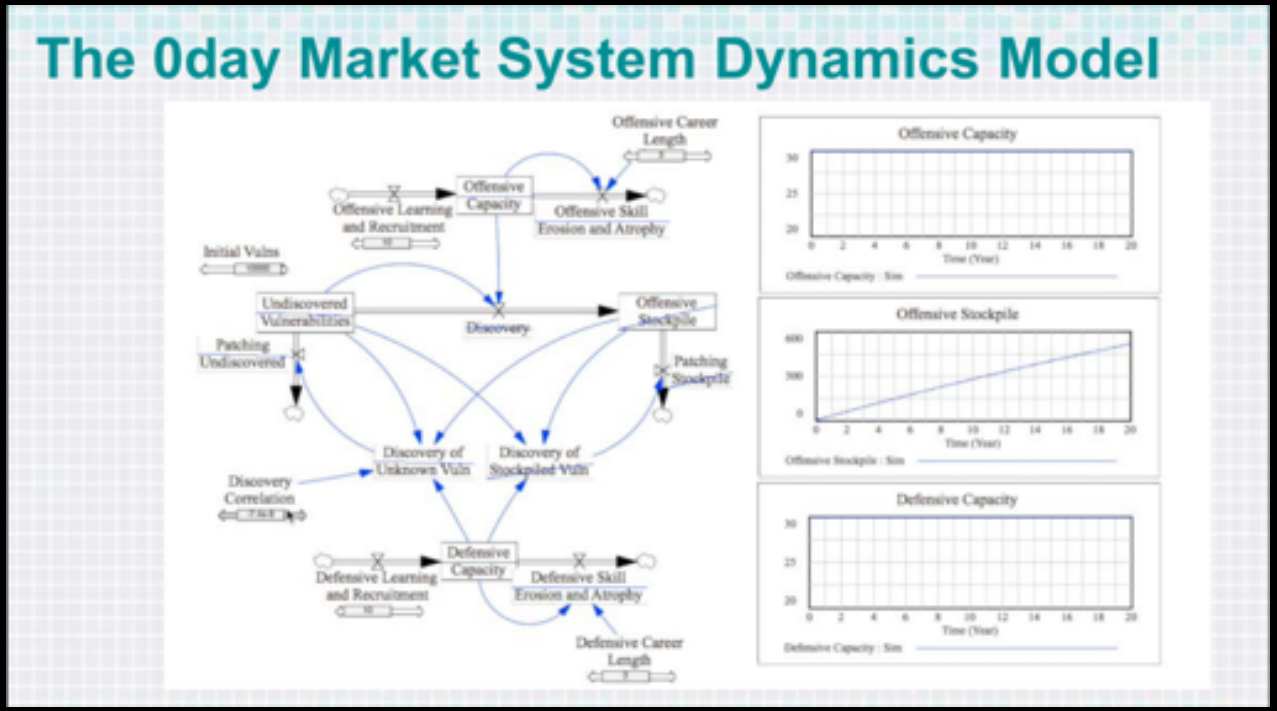
I left my full time jobs to do this full time in 2017. But I have been considering going back to a real job over the last few months. Garenteed money (even if less) is better sometimes than the unknown we face. And there are still thousands of other programs to look at

1 7

In the End, All We Have is Love



There is More To This Than Money



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

"The Wolves of Vuln Street"[3]

CLAIM: “Bug bounties have hundreds of thousands of friendly hackers for ‘continuous coverage’.”

0.03% made $100K or more
0.3% made $5K or more

BOUNTY REAL TALK

Noise vs skill

On 1 “leading platform”*:

- Over 300,000 hackers have signed up
- about 1 in 10 have found something to report;
- of those who have filed a report, a little over a quarter have received a bounty;
- 1,000 hackers have earned $5,000 or more;
- about 100 hackers have earned $100,000 or more; and
- two hackers have reached or are very close to $1 million in total rewards

97.5% never sold a bug

*https://www.techrepublic.com/article/bug-bounty-programs-everything-you-thought-you-knew-is-wrong/

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 that change over time**

TRUTH: The Defense Market for bugs can only go so high & there is a FINITE skilled labor market

Perverse Incentives

And ways to avoid them

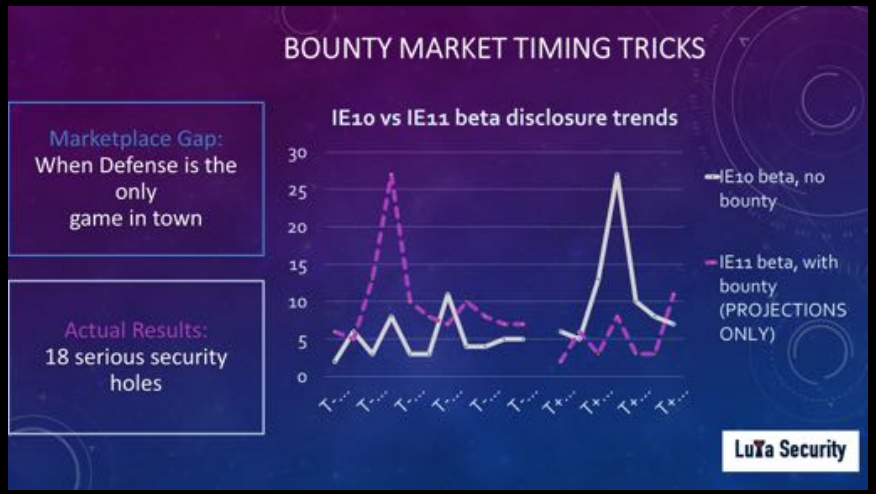
One Meeeeelion Dollars$$$$$$$$$$!!!

- Offense Prices Will Increase
- Collusion Risk Increases
- Interferes with Attraction & Retention of Employees

https://www.darkreading.com/vulnerabilities---threats/apples-new-bounty-program-has-huge-incentives-big-risks/d/d-id/1335517

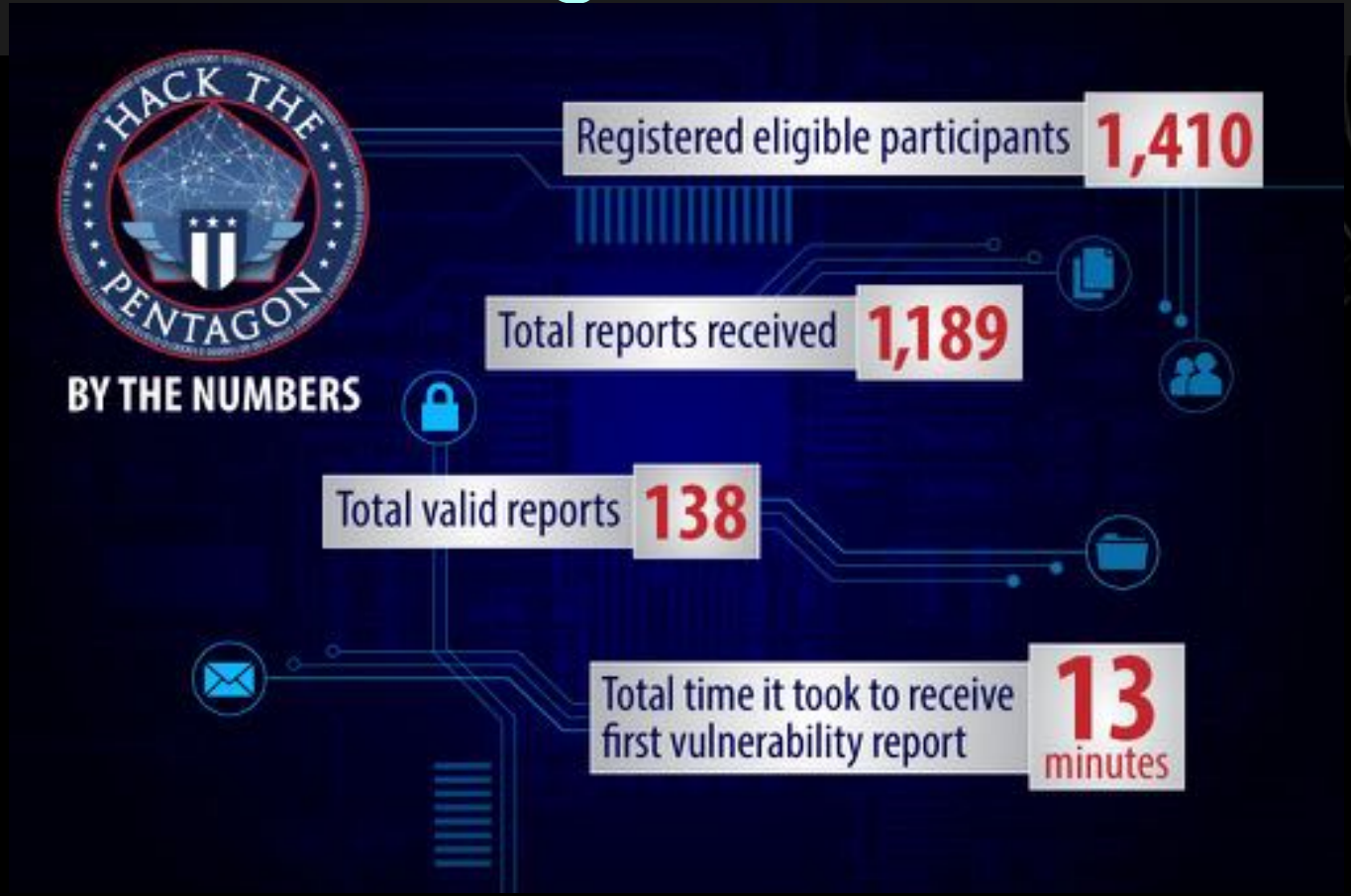
Perverse Incentives – Lessons from 1995

Know Your Bugs, Know Your Market, Know Your Audience



Bounty Smarter, Not Harder

Hack the Pentagon – Hack the Planet!




Hack the Army – Hack the Planet!
HACK THE
U.S.ARMY

Hack The Army – Gently With a Chainsaw


Hacking the Security Labor Market
Balancing defense, offense, prevention, maintenance

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”[2]
- Tiny fraction of talent; Majority generate **noise**
- Bug bounty hunting celebrated for outpacing median developer salaries (16x in India, 40x in Argentina)?!
- Top 10 CS programs in US universities don’t require security to graduate. 3/10 lack security electives.

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

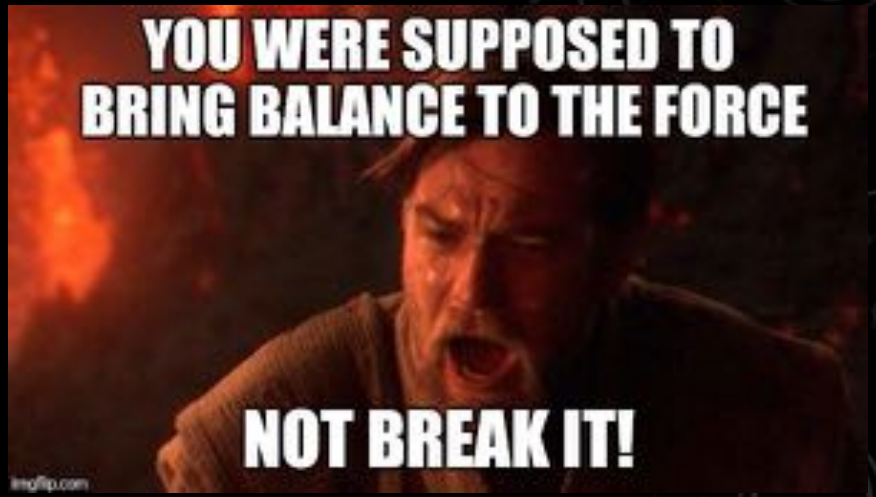
Data privacy, unless you've really spent time thinking through & planning for in-scope & out-of-scope scenarios

Go Hack Yourself, Then Hack Your Labor

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

Bug Bounty Botox: Not A Good Look!

In All Things, BALANCE



Creation, Maintenance, Destruction

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

Expand Your Labor Market
All Hands On Deck