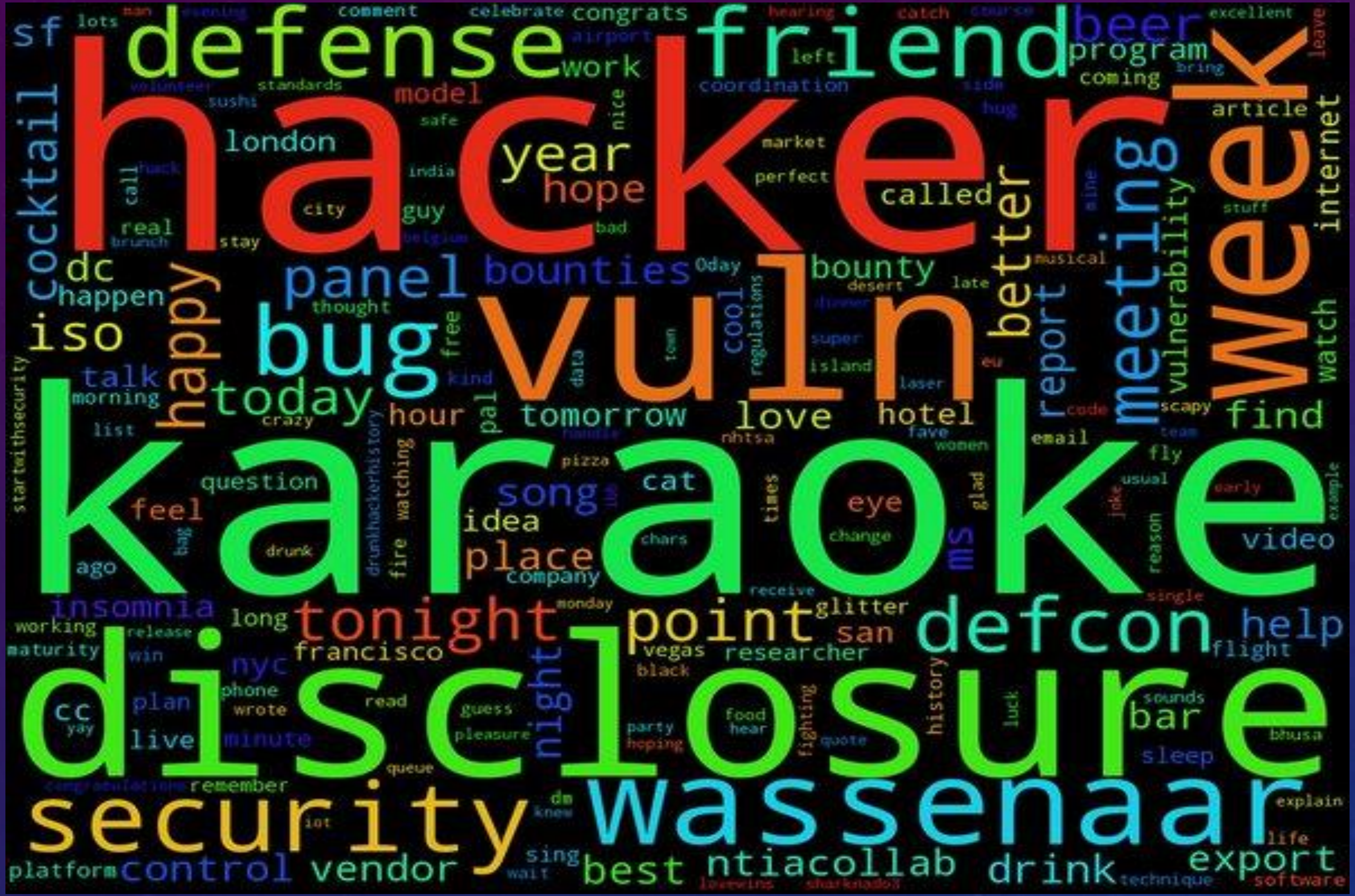
CROUCHING TIGER SUDDEN KEYNOTE

IN DATA WE TRUST

KATIE MOUSSOURIS

LUTA SECURITY

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

LUTA SECURITY

@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

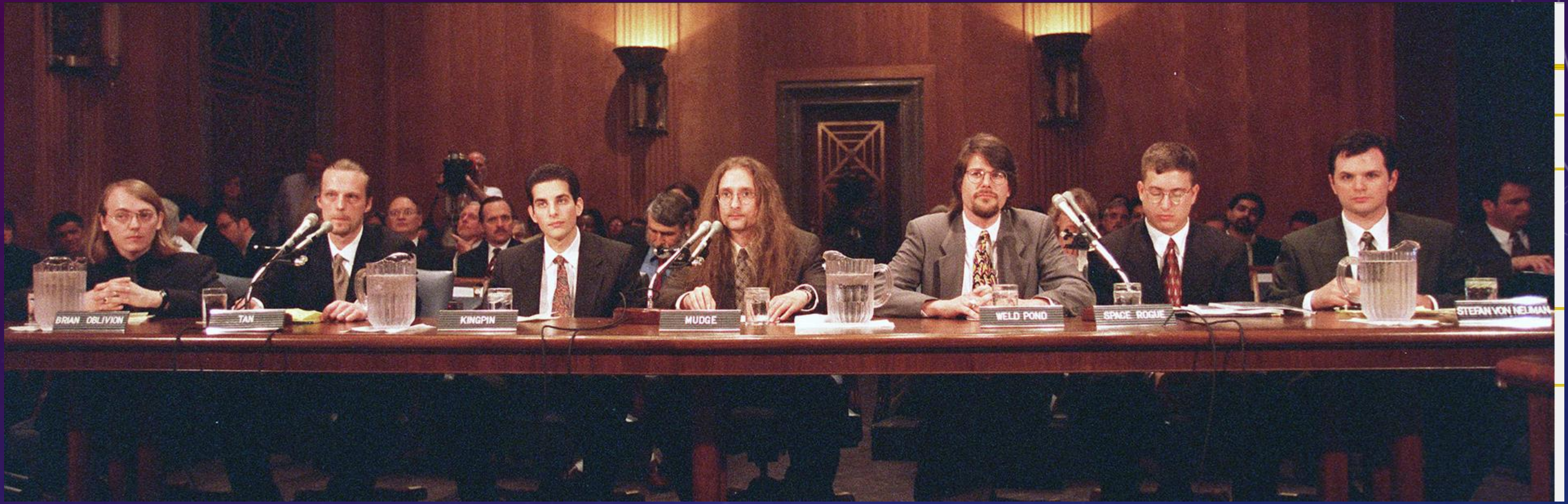
Testifying before US Senate on Uber Data Breach Bounty Coverup

Making T-Rex Arms on CSPAN[1]

The picture I send to my family to explain my job

LUTA SECURITY

HACKERS HAVE BEEN WARNING US FOR DECADES



L0pht Hacking Group Testifying Before US Congress in 1998 about the Internet’s Fragility

AKA: The l0pht Supper, In Mudge We Trust

20 YEARS LATER…WE STILL HAVE A PROBLEM …& HAIR

LUTA SECURITY

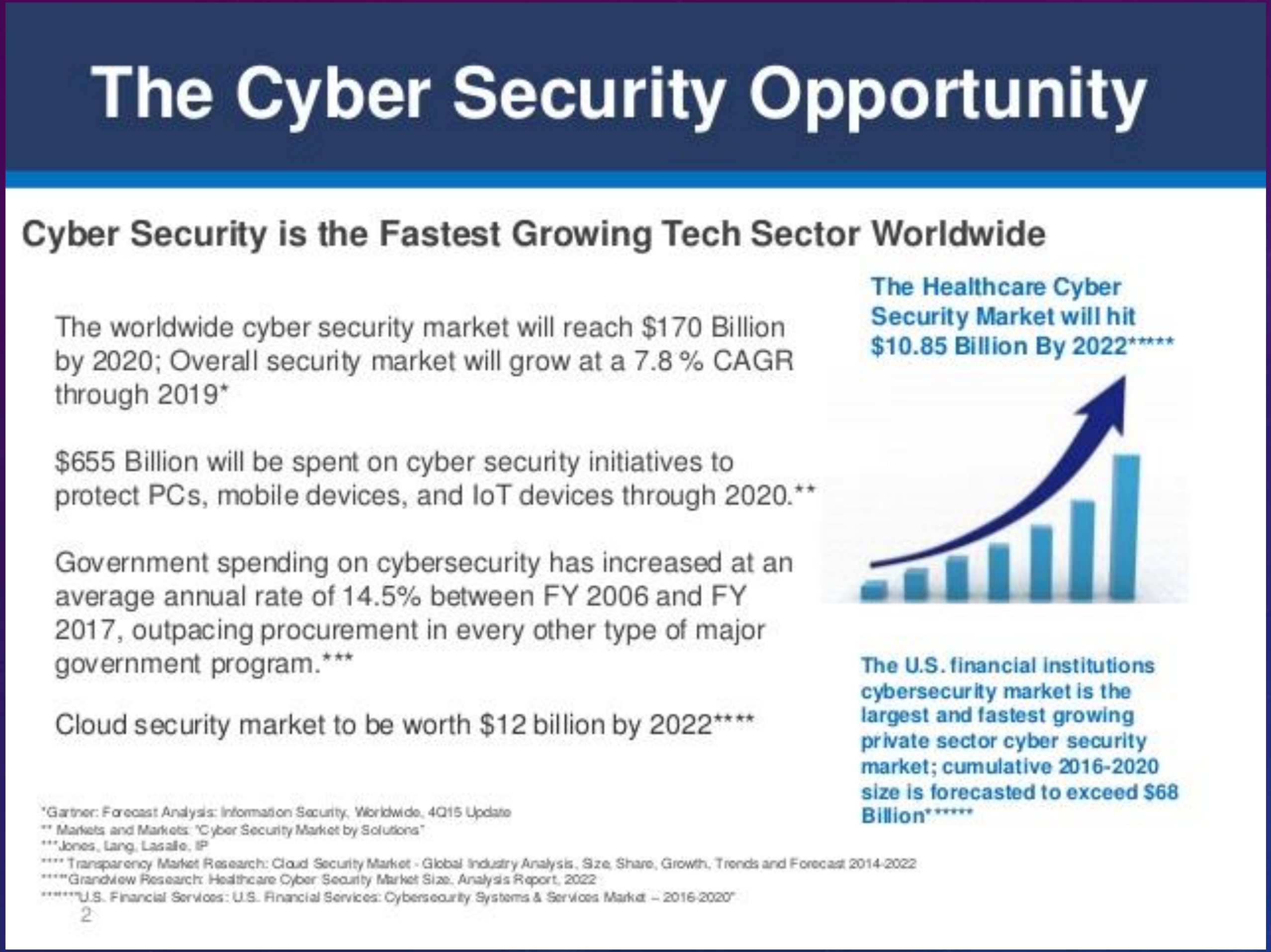
Photos courtesy of Deb Kavaler Wysopal

HOW DID WE GET HERE?

CAN’T WE JUST THROW MORE MONEY AT THIS PROBLEM?

SURPRISE!! MONEY CAN’T BUY YOU SECURITY

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.***

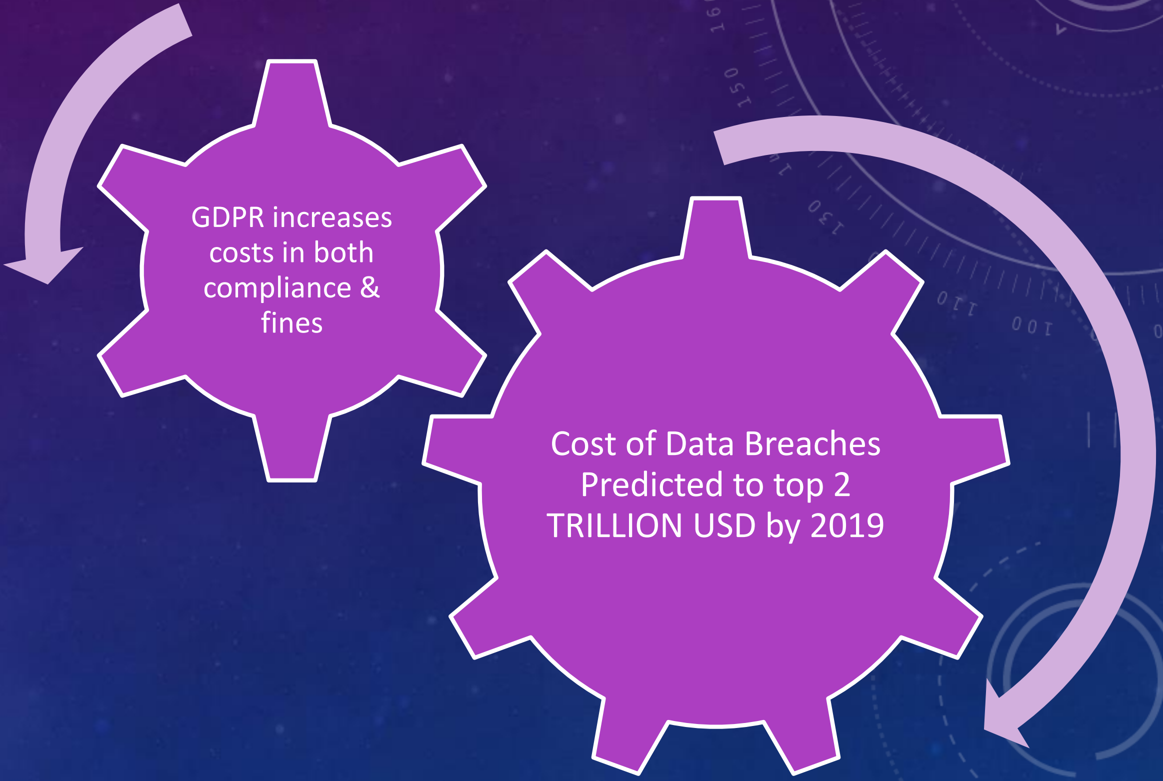
Cloud security market to be worth $12 billion by 2022****

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"

2



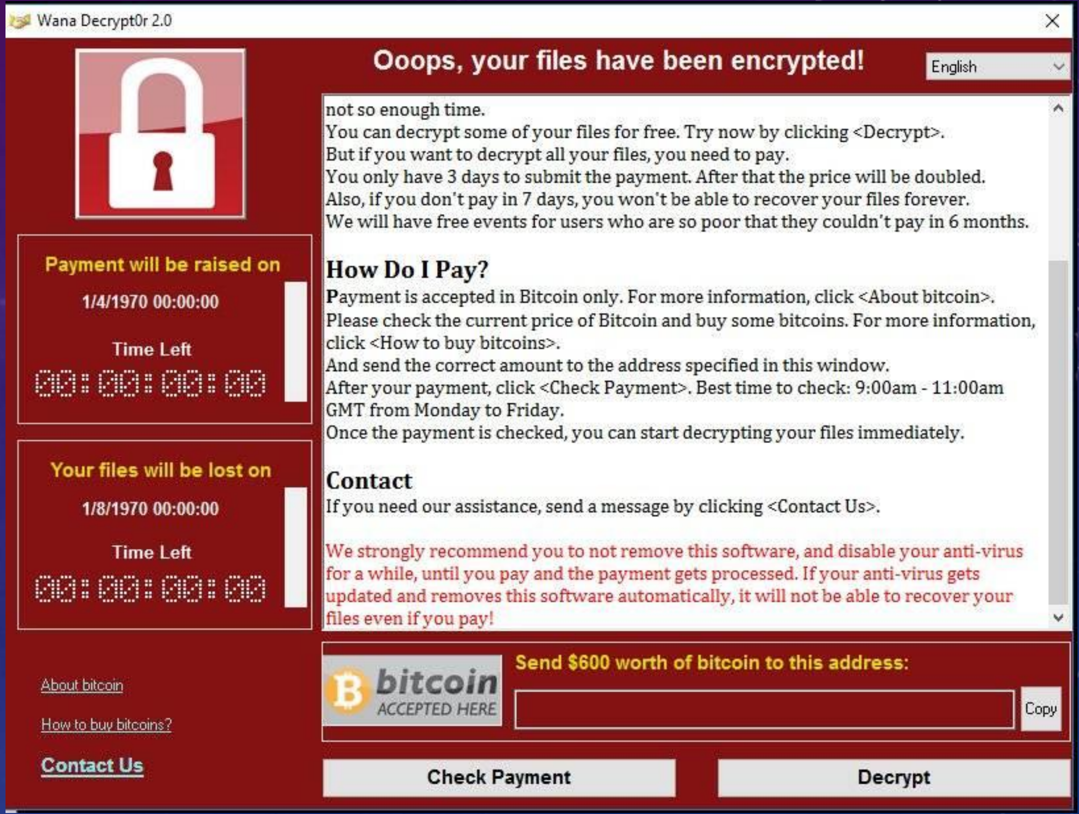
GDPR increases costs in both compliance & fines

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

SILVER BULLETS ARE FOR WEREWOLVES

LUTA SECURITY

AND YET, HERE WE ARE



Ooops, your files have been encrypted!

not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.
Once the payment is checked, you can start decrypting your files immediately.

Contact

If you need our assistance, send a message by clicking <Contact Us>.

We strongly recommend you to not remove this software, and disable your anti-virus for a while, until you pay and the payment gets processed. If your anti-virus gets updated and removes this software automatically, it will not be able to recover your files even if you pay!

Payment will be raised on
1/4/1970 00:00:00
Time Left
00:00:00:00

Your files will be lost on
1/8/1970 00:00:00
Time Left
00:00:00:00

About bitcoin
How to buy bitcoins?
Contact Us

bitcoin ACCEPTED HERE

Send $600 worth of bitcoin to this address:

Copy

Check Payment

Decrypt

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

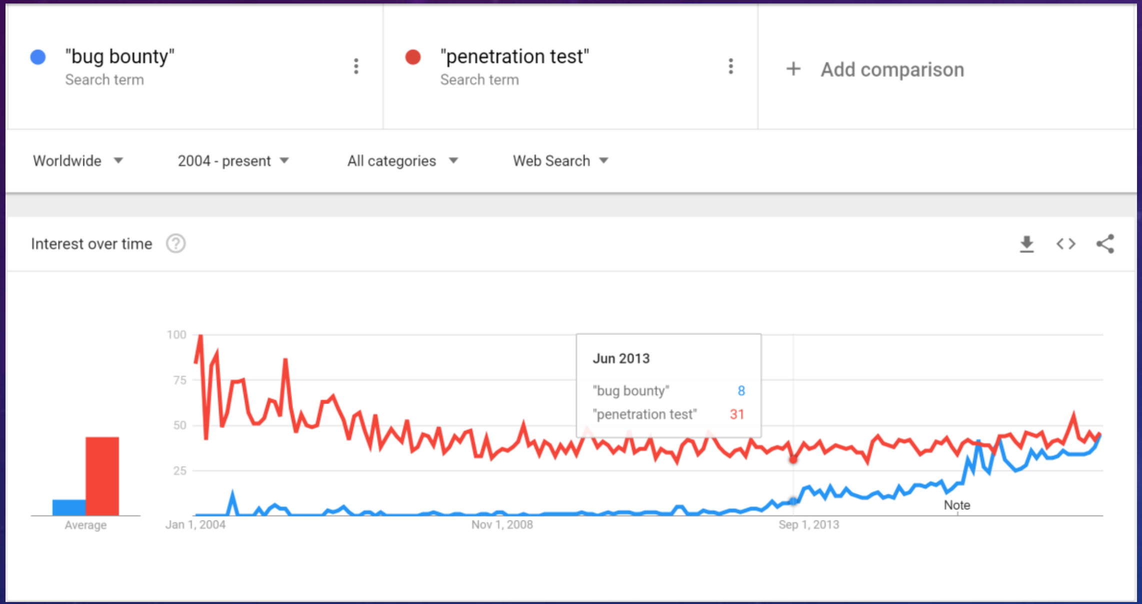
Increased Security Spending ≠ Increased Security

LUTA SECURITY

DON'T CONFLATE OR CONFUSE PEN TESTS WITH BUG BOUNTIES

Inflection Point #1:

Fitting Earths into Jupiter's Storm



● "bug bounty"
Search term

● "penetration test"
Search term

＋ Add comparison

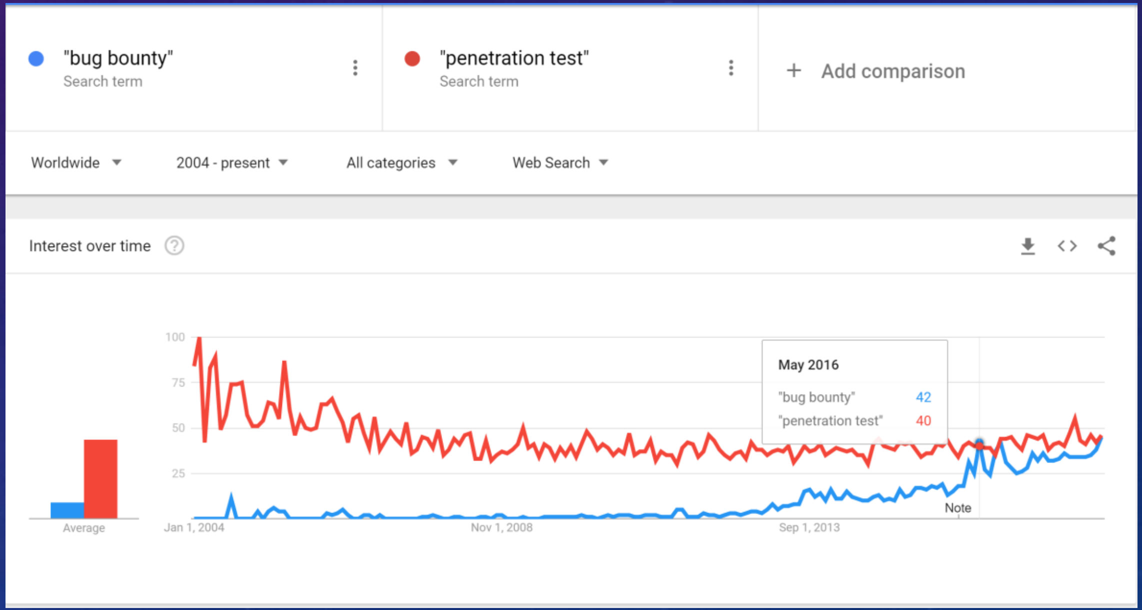
Worldwide ▾ 2004 - present ▾ All categories ▾ Web Search ▾

Interest over time

Jun 2013
"bug bounty" 8
"penetration test" 31

Inflection Point #2:

5 Sides to Every Story



● "bug bounty"
Search term

● "penetration test"
Search term

＋ Add comparison

Worldwide ▾ 2004 - present ▾ All categories ▾ Web Search ▾

Interest over time

May 2016
"bug bounty" 42
"penetration test" 40

LUTA
SECURITY

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.

LUTA SECURITY

EASY! LET'S JUST OPEN THE FRONT DOOR!

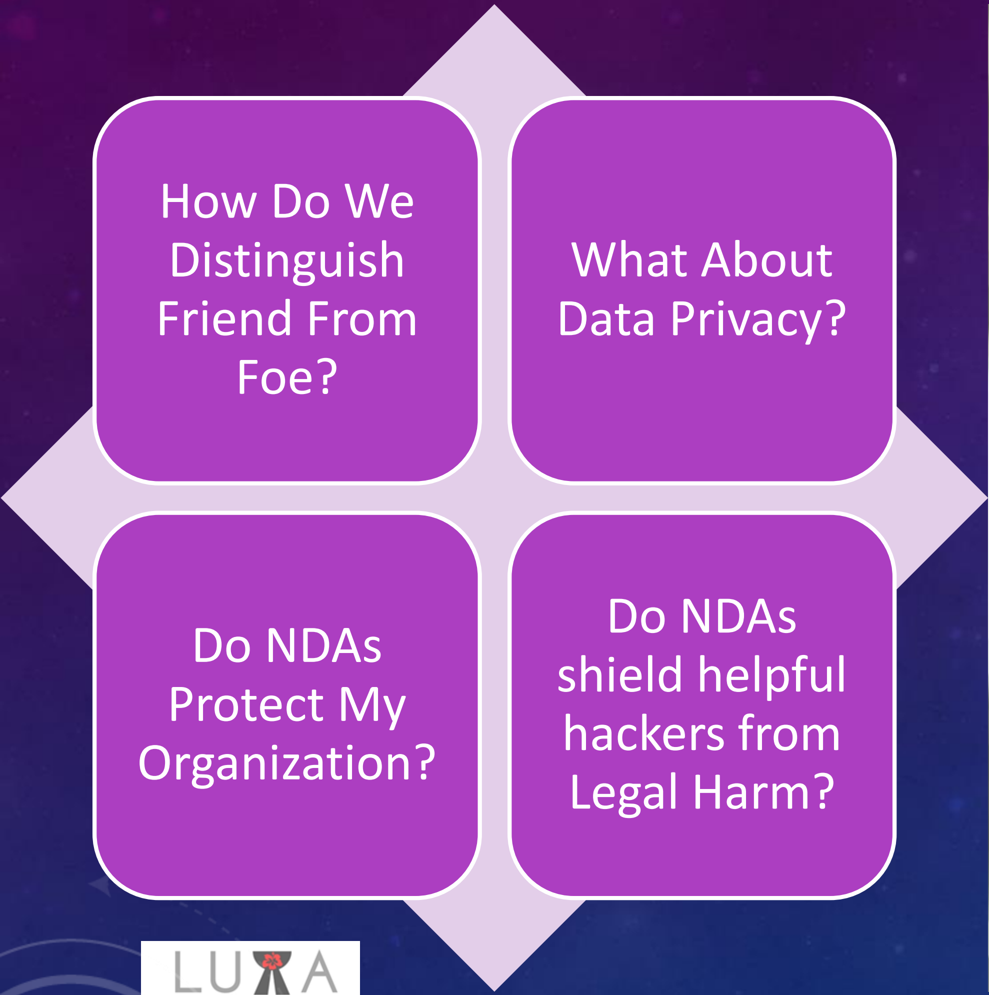
WE TAKE SECURITY VEWWY VEWWY SERIOUSLY! LET'S JUST START A BUG BOUNTY! WHAT COULD POSSIBLY GO WRONG?!!!111!! SURPRISE!! EVERYTHING.

LUTA SECURITY

Was This What You Were Expecting?

LURA SECURITY

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?

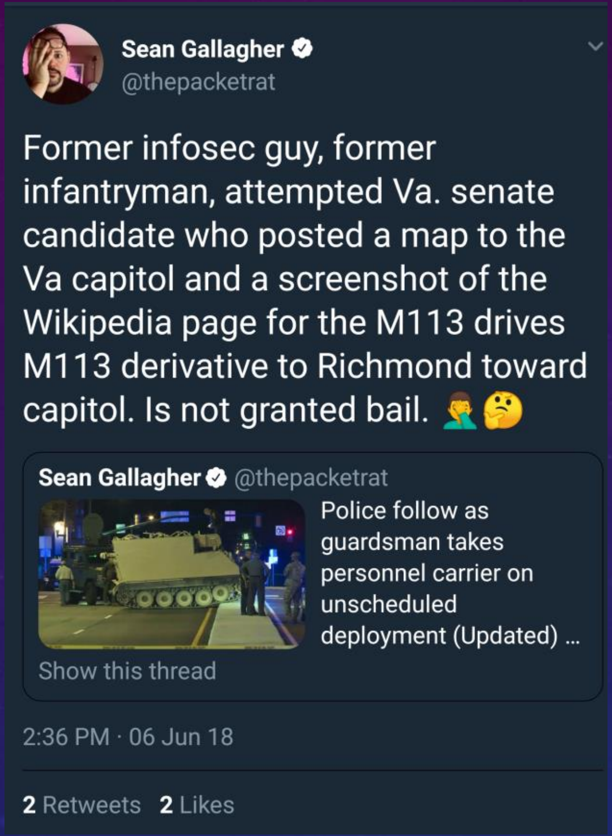
LUTA SECURITY

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?

LUTA SECURITY

TANK YOU FOR YOUR SERVICE



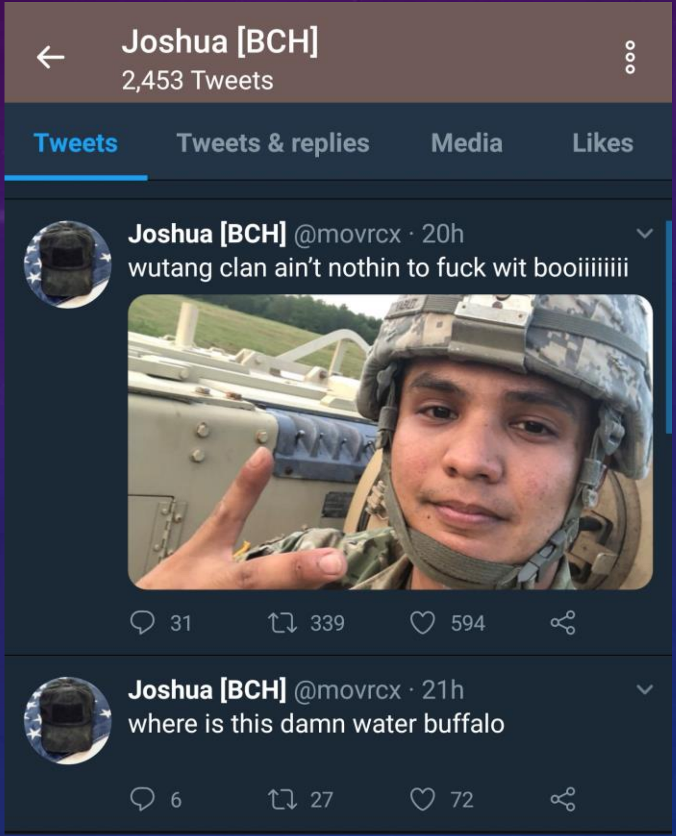
Sean Gallagher @thepacketrat

Former infosec guy, former infantryman, attempted Va. senate candidate who posted a map to the Va capitol and a screenshot of the Wikipedia page for the M113 drives M113 derivative to Richmond toward capitol. Is not granted bail. 🤦‍♂️🤔

> **Sean Gallagher** @thepacketrat
> Police follow as guardsman takes personnel carrier on unscheduled deployment (Updated) ...
> Show this thread

2:36 PM · 06 Jun 18

2 Retweets **2** Likes

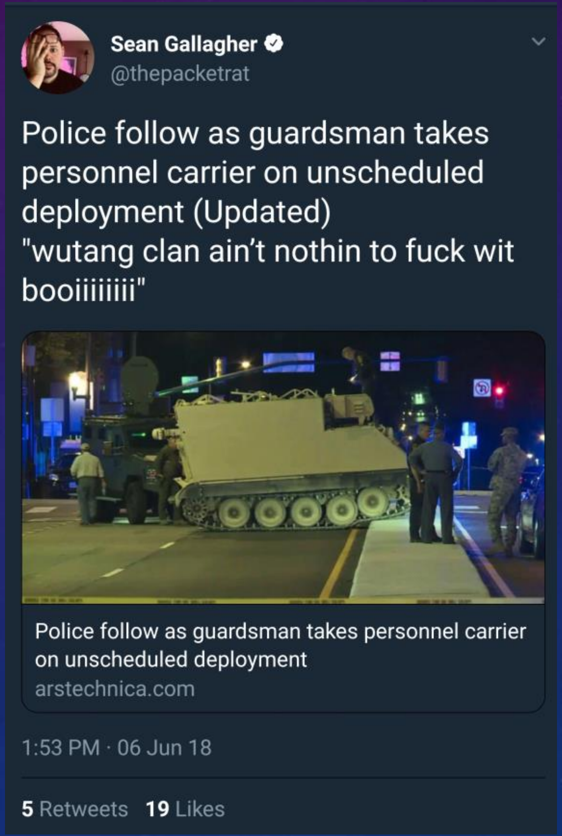


Joshua [BCH] @movrcx · 20h
wutang clan ain't nothin to fuck wit booiiiiiiii

31 339 594

Joshua [BCH] @movrcx · 21h
where is this damn water buffalo

6 27 72



Sean Gallagher @thepacketrat

Police follow as guardsman takes personnel carrier on unscheduled deployment (Updated)
"wutang clan ain't nothin to fuck wit booiiiiiiii"

> Police follow as guardsman takes personnel carrier on unscheduled deployment
> arstechnica.com

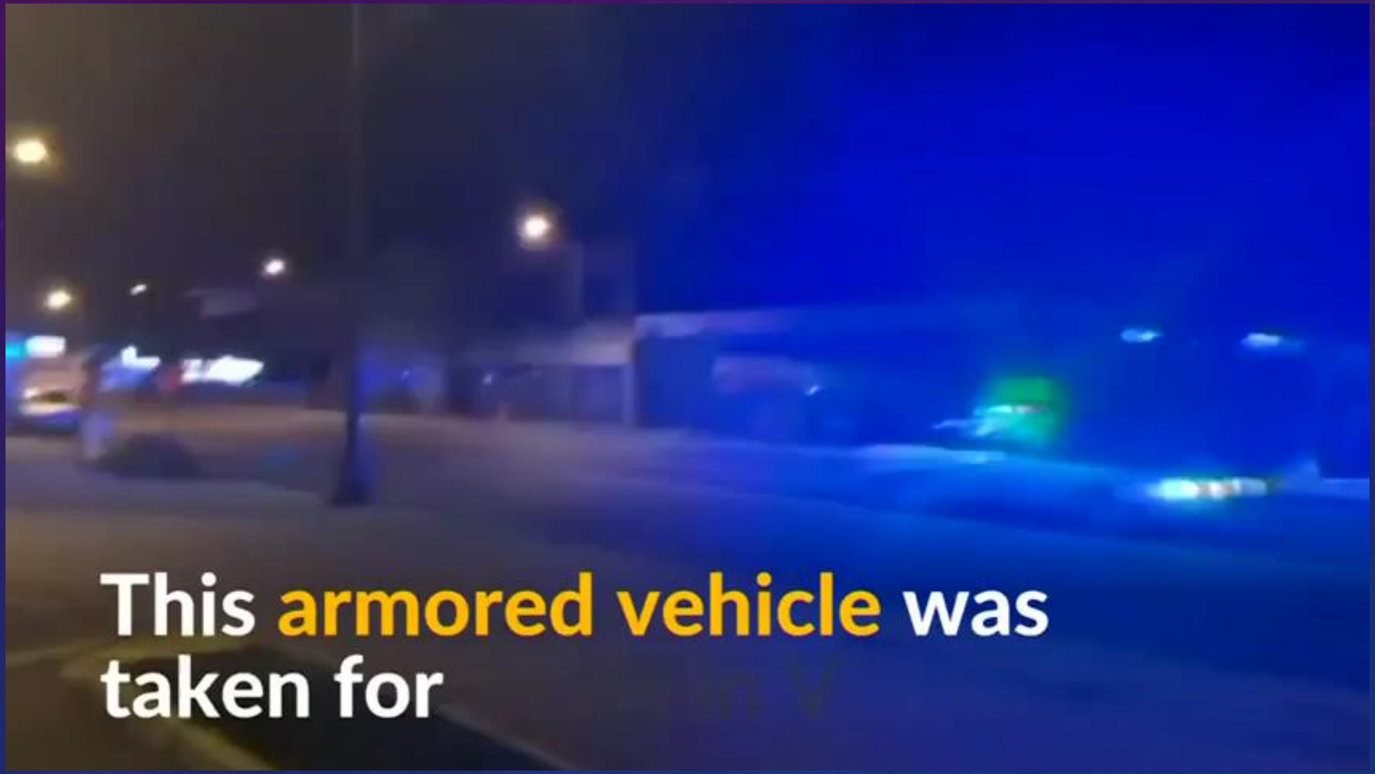
1:53 PM · 06 Jun 18

5 Retweets **19** Likes

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!!!



LURA SECURITY

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

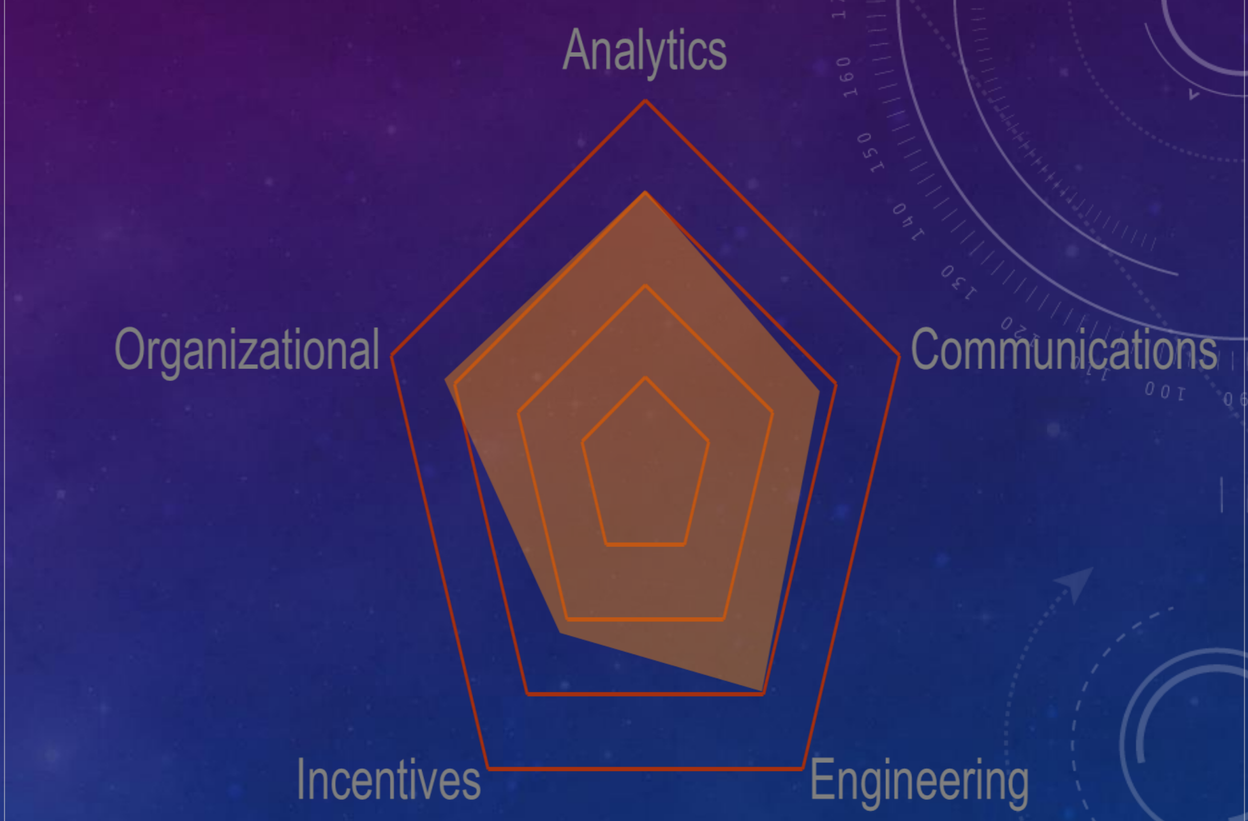
Capacity Planning & Maturity is the Right Way Forward

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

LUTA SECURITY

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



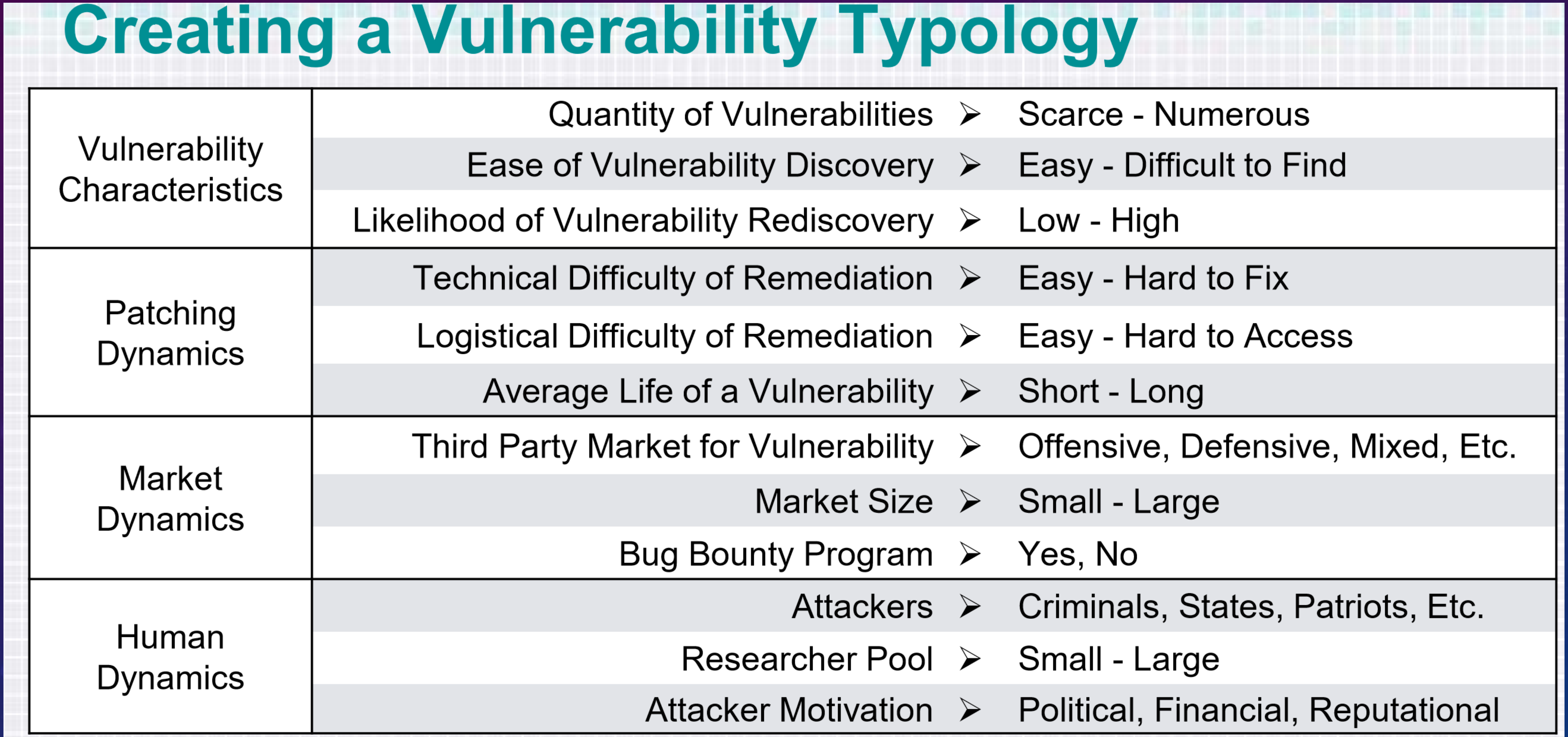
LUTTA SECURITY

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

LUTA
SECURITY

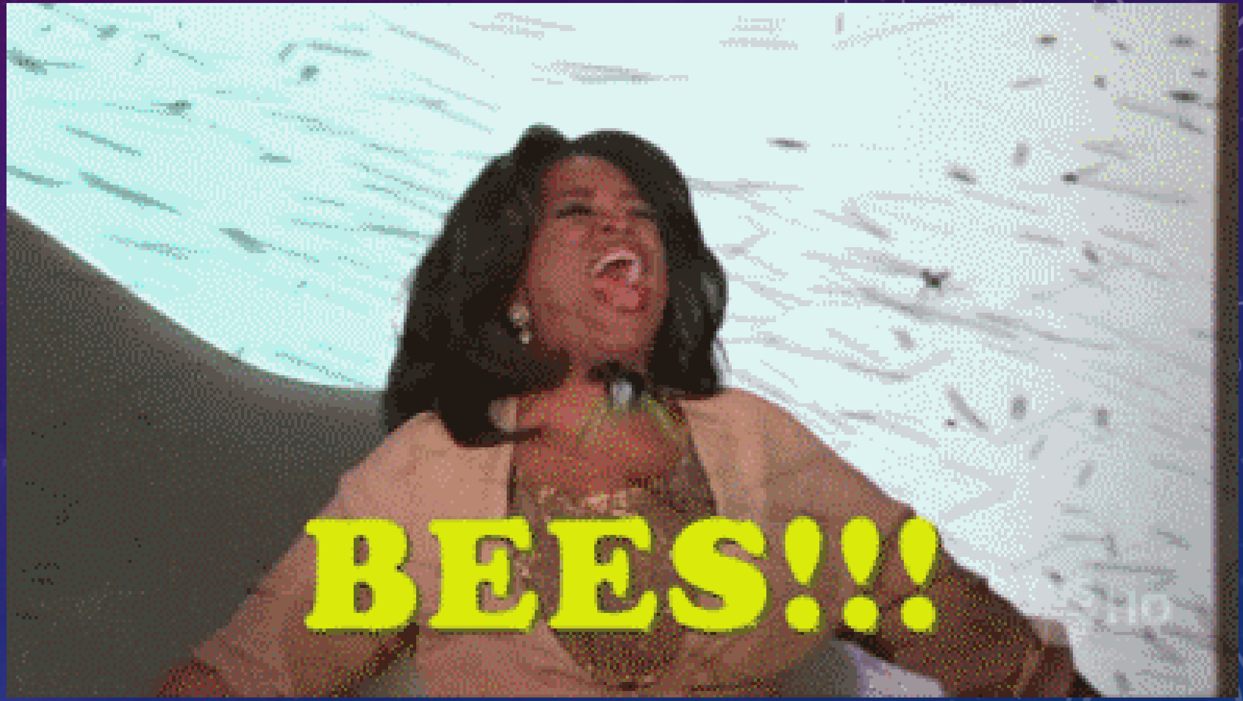
#NOTALLBUGS ARE CREATED (OR FIXED) EQUALLY



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.

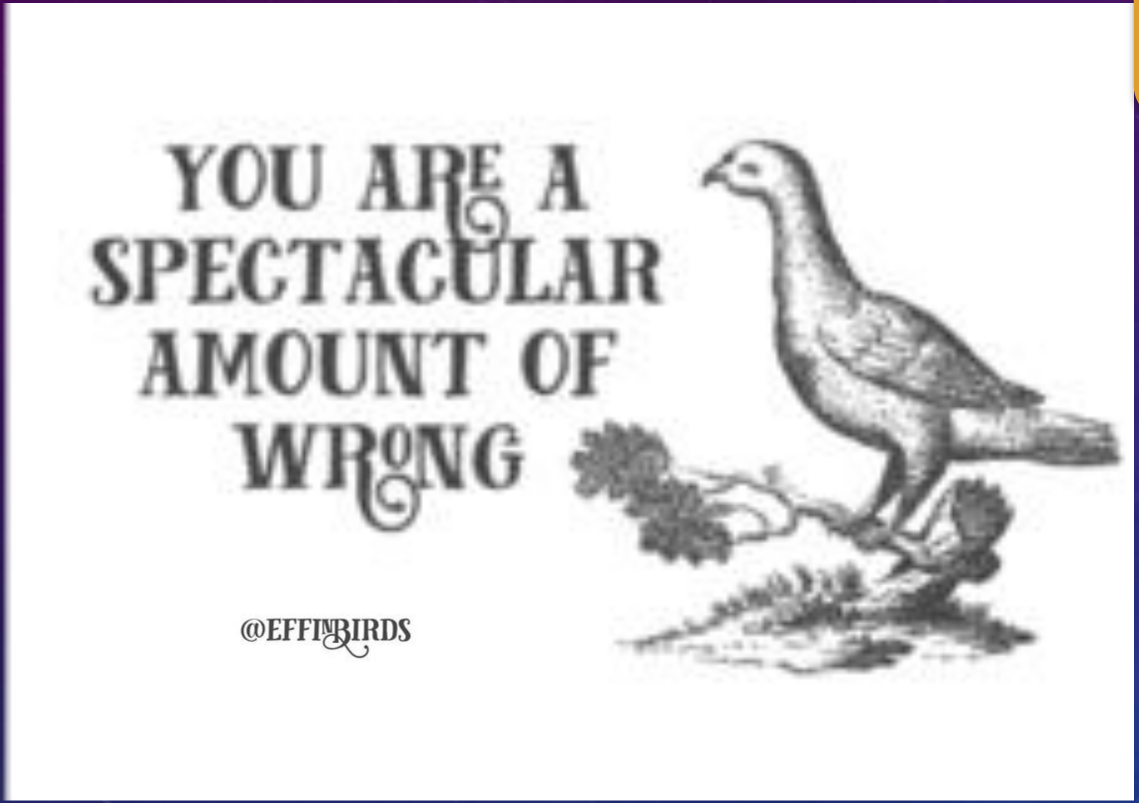
LUTA SECURITY

MYTHS, MOTIVATIONS, & MARKETS

OR, RAISE YOUR HAND WHOMEVER HASN’T BROKEN ANY LAWS

LUTA
SECURITY

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**

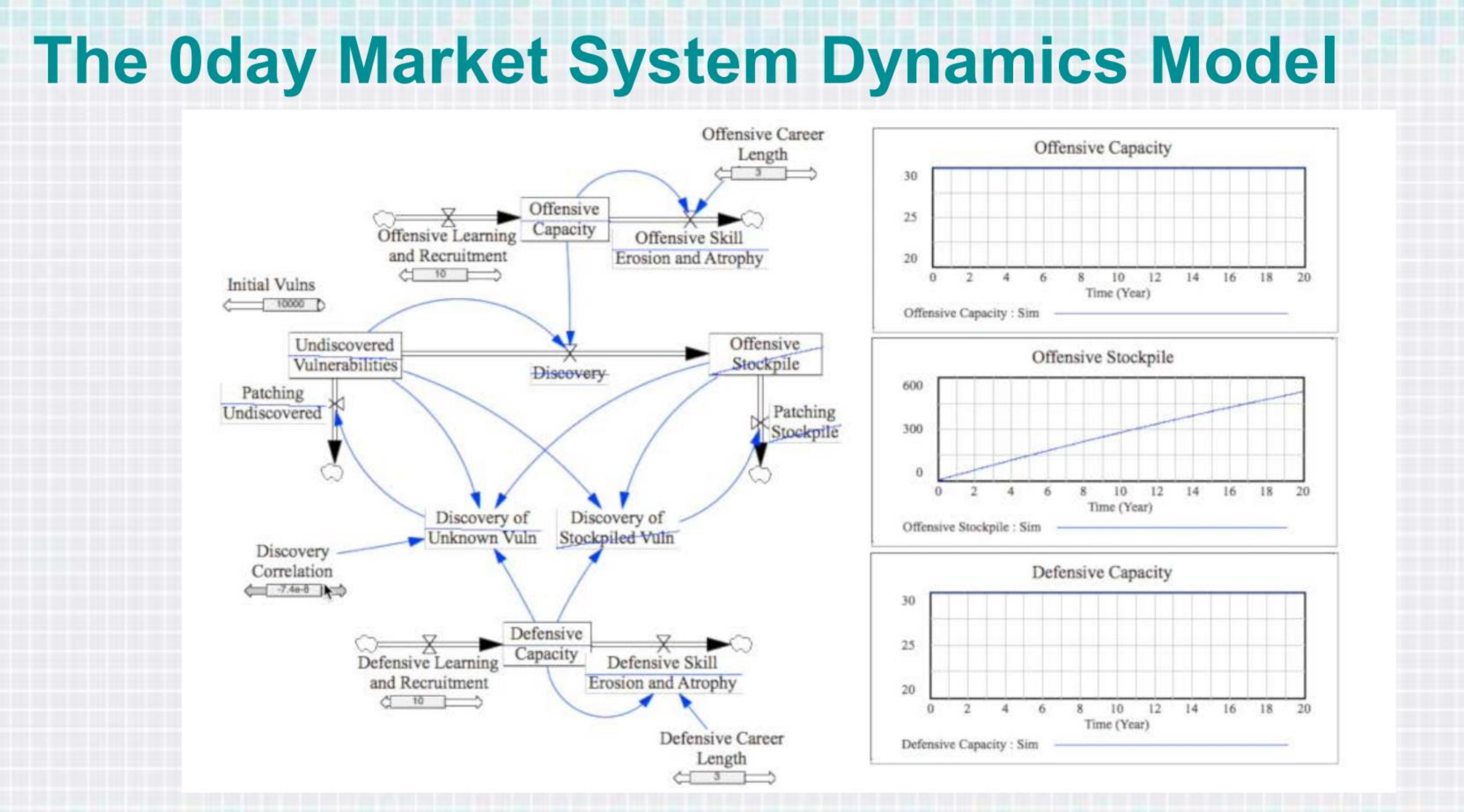
LUTA SECURITY

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:

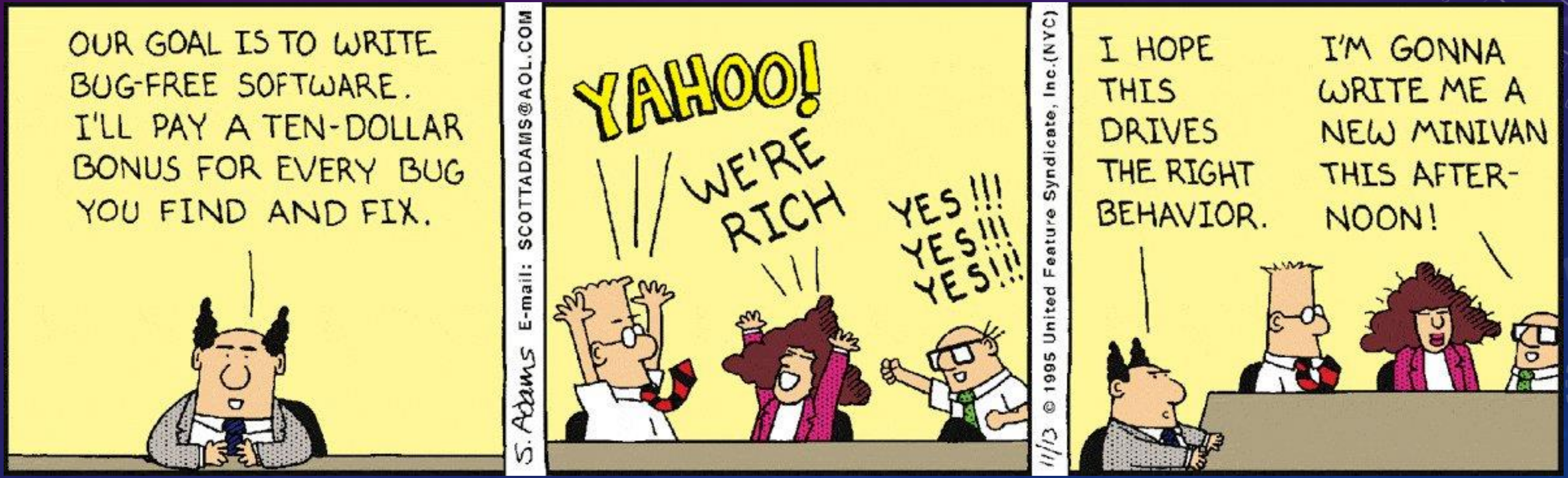
"The Wolves of Vuln Street"[3]

PERVERSE INCENTIVES

AND WAYS TO AVOID THEM

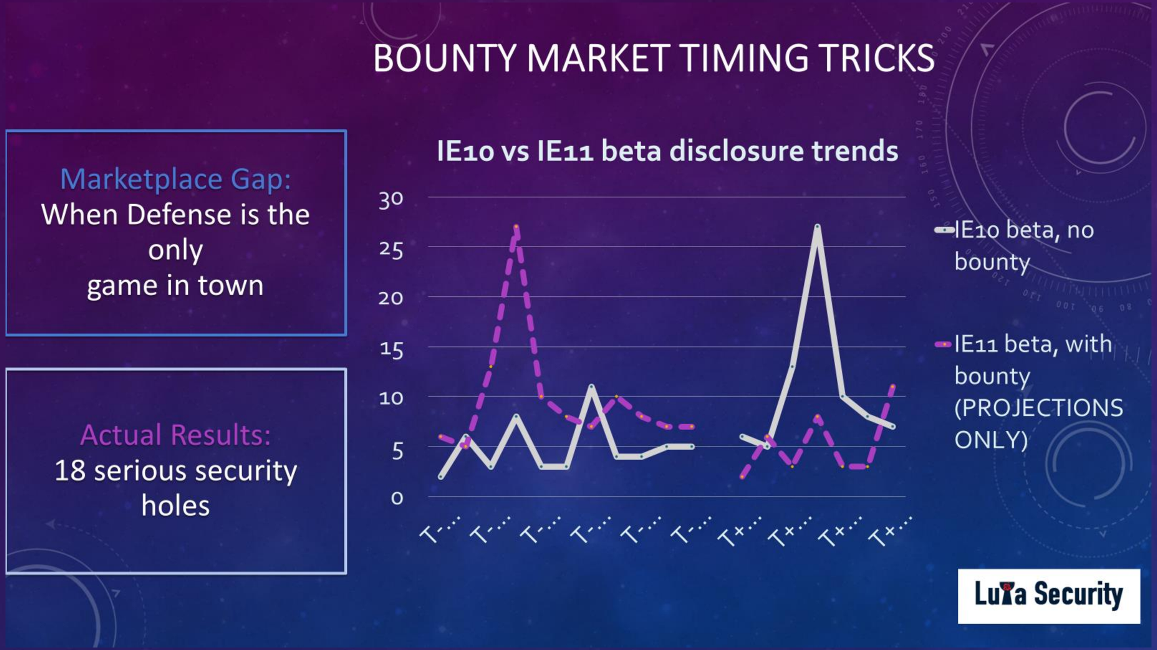
LUTA SECURITY

PERVERSE INCENTIVES – LESSONS FROM 1995


OUR GOAL IS TO WRITE BUG-FREE SOFTWARE. I'LL PAY A TEN-DOLLAR BONUS FOR EVERY BUG YOU FIND AND FIX.
S. Adams E-mail: SCOTTADAMS@AOL.COM
YAHOO!
WE'RE RICH
YES!!! YES!!! YES!!!
11/13 © 1995 United Feature Syndicate, Inc.(NYC)
I HOPE THIS DRIVES THE RIGHT BEHAVIOR.
I'M GONNA WRITE ME A NEW MINIVAN THIS AFTER-NOON!

LUTA SECURITY

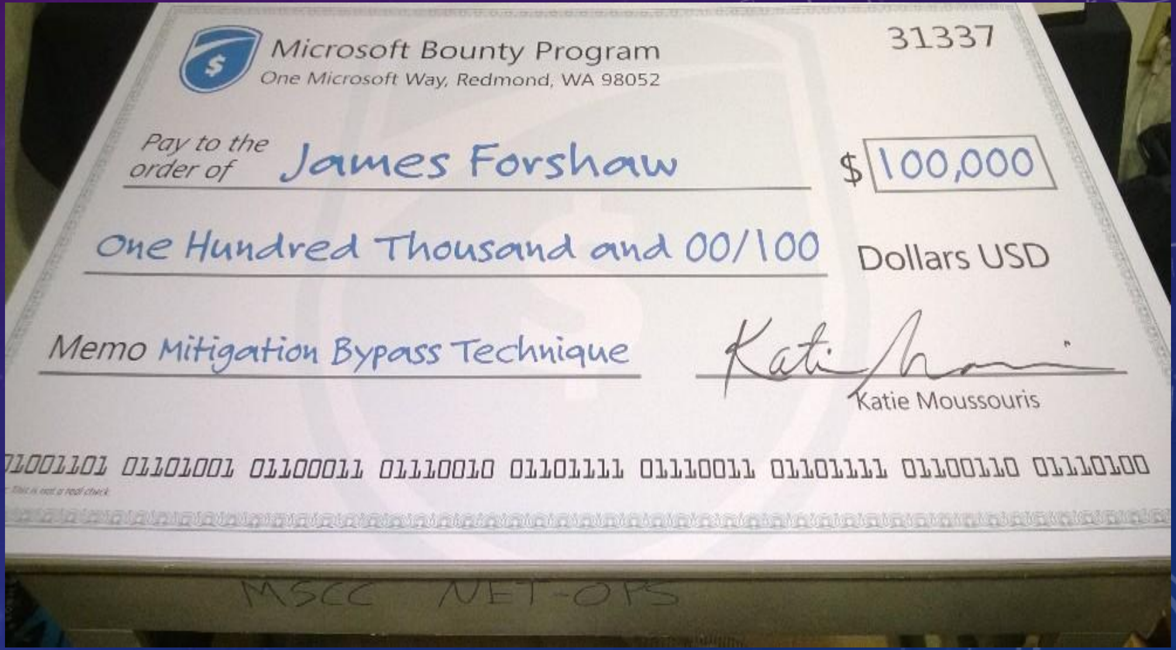
Know Your Bugs, Know Your Market, Know Your Audience



BOUNTY MARKET TIMING TRICKS

Marketplace Gap: When Defense is the only game in town

Actual Results: 18 serious security holes



Microsoft Bounty Program
One Microsoft Way, Redmond, WA 98052

31337

Pay to the order of James Forshaw $ 100,000

One Hundred Thousand and 00/100 Dollars USD

Memo Mitigation Bypass Technique

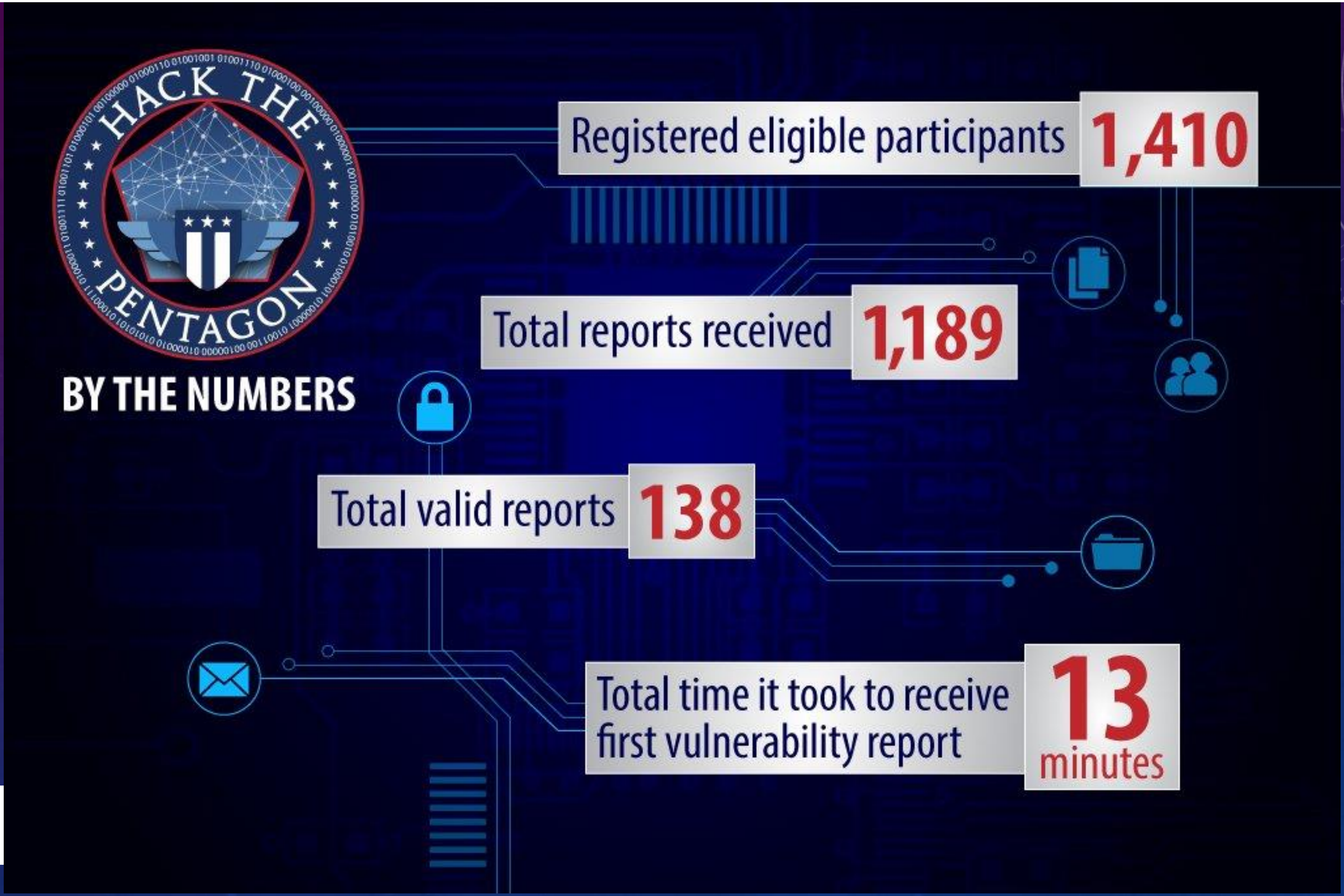
Katie Moussouris

1001101 01101001 01100011 01110010 01101111 01110011 01101111 01100110 01110100

This is not a real check

BOUNTY SMARTER, NOT HARDER

HACK THE PENTAGON – HACK THE PLANET!



BY THE NUMBERS

Registered eligible participants 1,410

Total reports received 1,189

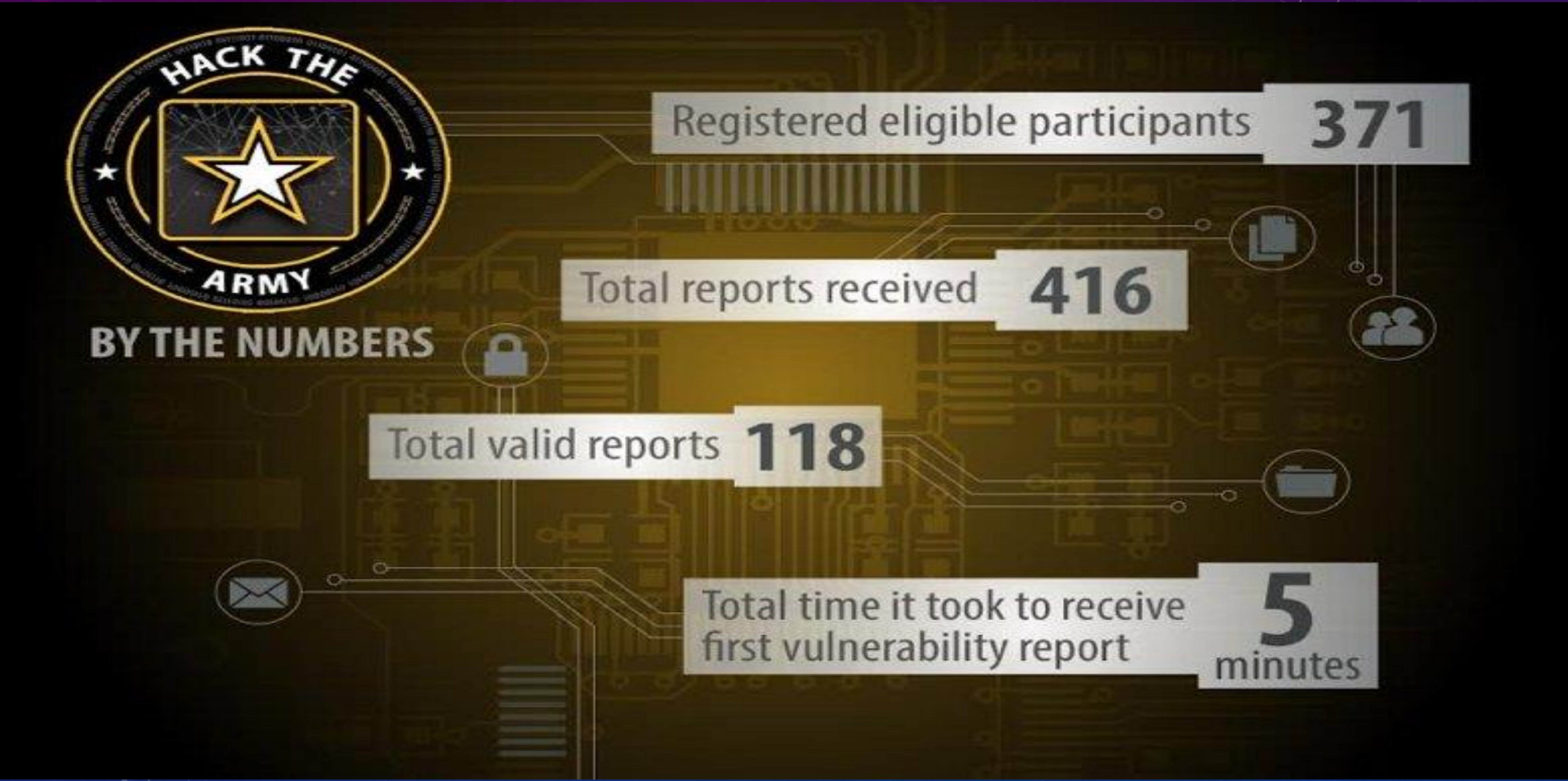
Total valid reports 138

Total time it took to receive first vulnerability report 13 minutes

LUTA SECURITY

Hack the Army – Hack the Planet!

Hack The Army – Gently With a Chainsaw



HACK THE ARMY

BY THE NUMBERS

Registered eligible participants **371**

Total reports received **416**

Total valid reports **118**

Total time it took to receive first vulnerability report **5** minutes

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.

LUTA
SECURITY

LABOR MARKET FOR BUG HUNTING & FIXING ARE BEING SHAPED RIGHT NOW

AND IT’S COMING FROM INSIDE THE HOUSE! AND THE SENATE!! AND THE EU COMMISSION!!!!

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.

LUTA SECURITY

I KNOW! LET'S JUST PASS A LAW THAT SAYS "BE SECURE!"

"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**."

LUTA SECURITY

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

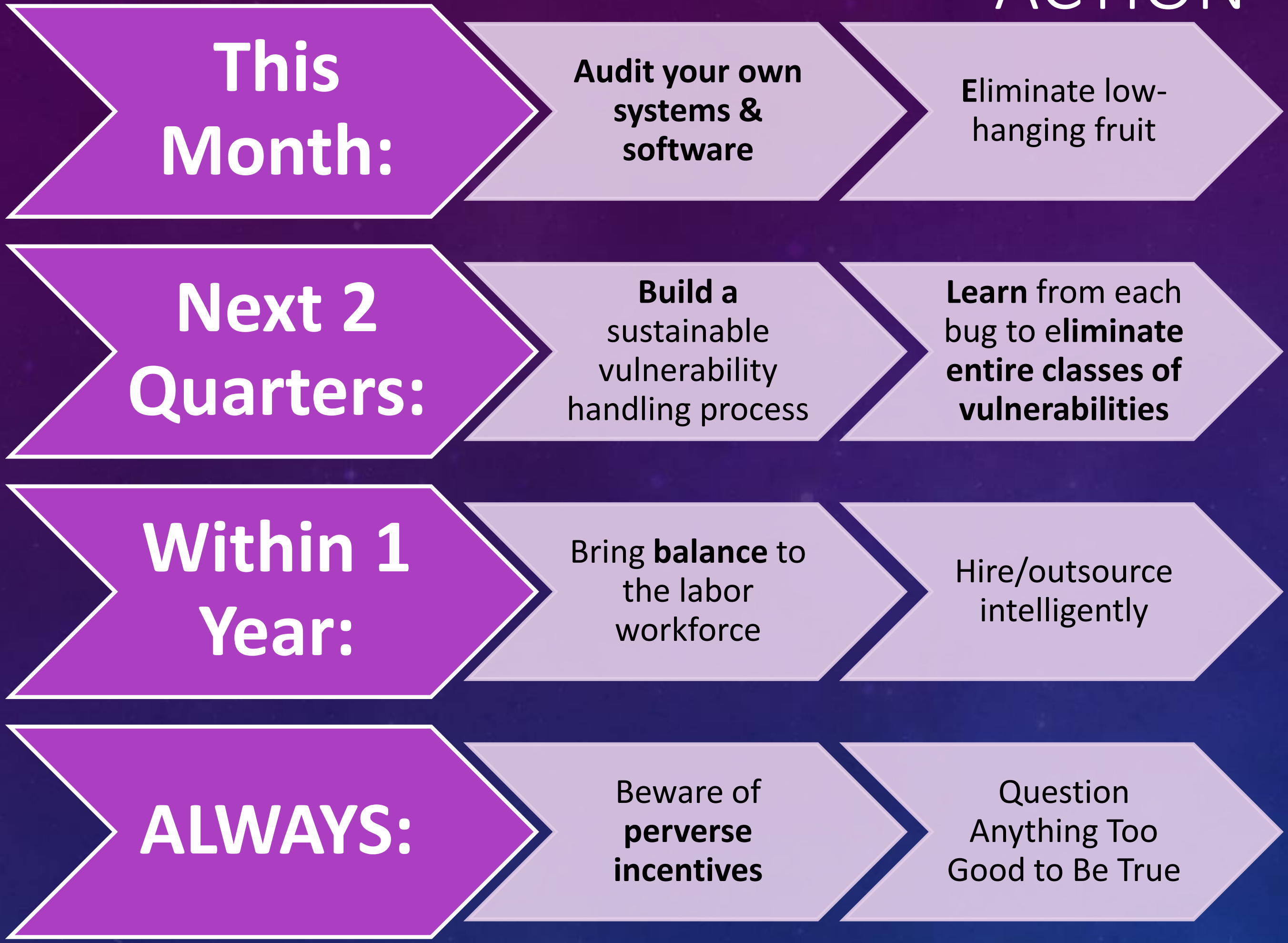
Your First External Bug Reports (unless you are teeny tiny!)

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

LUTA SECURITY

MEDITATE ON THE WABI SABI WORLD WIDE WEB – AND TAKE ACTION



This Month:

Audit your own systems & software

Eliminate low-hanging fruit

Next 2 Quarters:

Build a sustainable vulnerability handling process

Learn from each bug to **eliminate entire classes of vulnerabilities**

Within 1 Year:

Bring **balance** to the labor workforce

Hire/outsource intelligently

ALWAYS:

Beware of **perverse incentives**

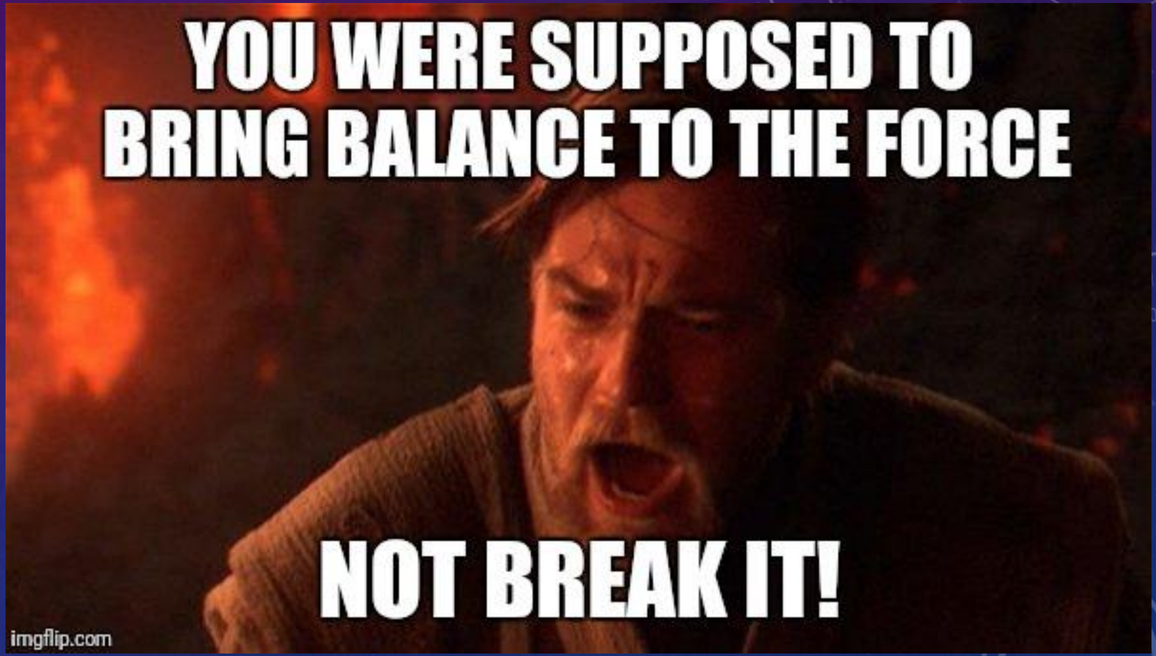
Question Anything Too Good to Be True

LUTA SECURITY

In All Things, BALANCE

LORD BRAHMA
LORD VISHNU
LORD SHIVA

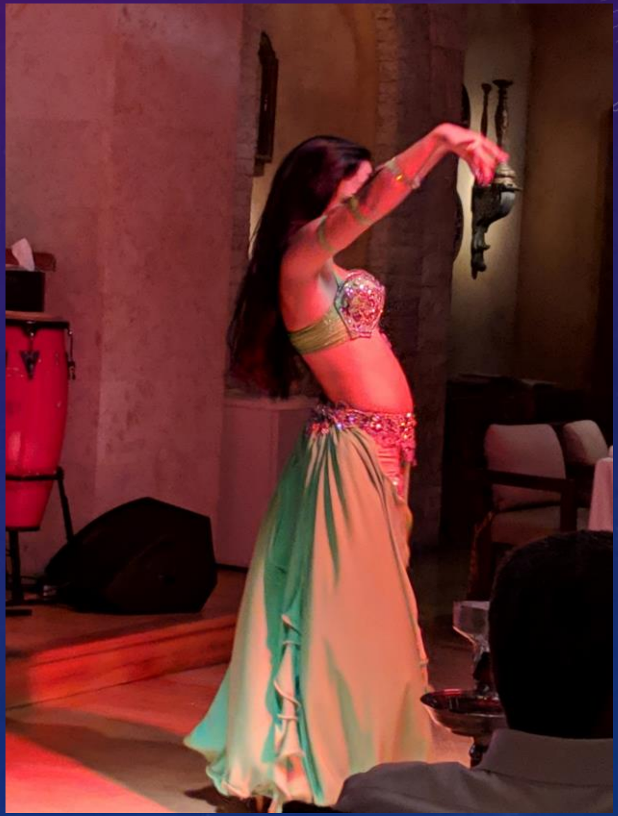
In Hinduism, the "Trimurti" 'three forms' - is a concept in Hinduism "in which the cosmic functions of creation, maintenance, and destruction are personified by the forms of Brahma the creator, Vishnu the maintainer or preserver, and Shiva the destroyer or transformer." These three deities have been called "the Hindu triad" or the "Great Trinity". Of the three members of the Trimurti, the Bhagavata Purana, which espouses the Vaishnavite viewpoint, explains that the greatest benefit can be had from Vishnu.



CREATION, MAINTENANCE, DESTRUCTION

LUTA SECURITY

DANCING THROUGH THE RHYTHMS OF EVOLUTION



LUTA SECURITY

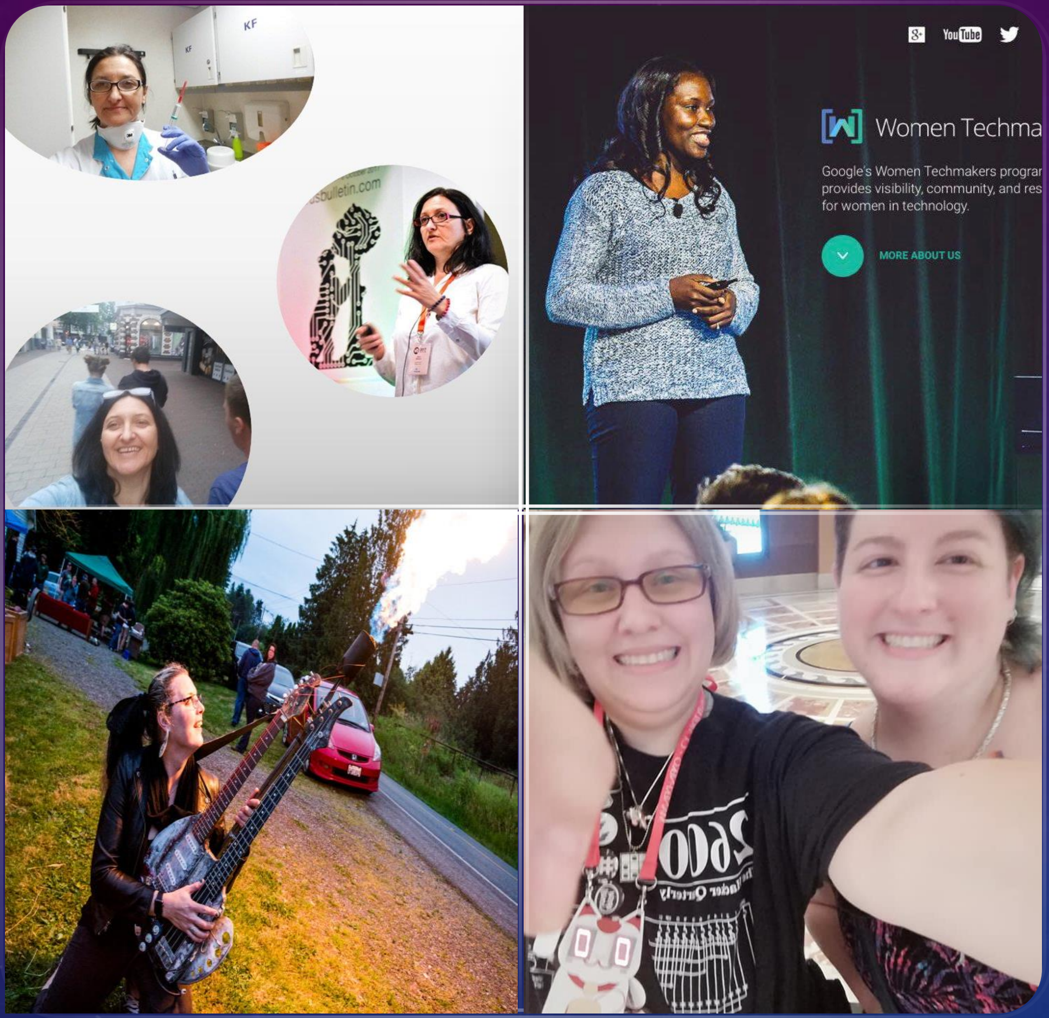
REFERENCES.

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

THE FUTURE IS HERE: SURPRISE ME!


Women Techma
Google's Women Techmakers progra
provides visibility, community, and res
for women in technology.
MORE ABOUT US
2600

LUTA
SECURITY