Bug Bounties & VDPs

Lessons Learned From Industry

NIST

KATIE MOUSSOURIS

CEO & FOUNDER, LUTA SECURITY

About Luta Security

- **Company:** Luta Security is transforming the way governments and organizations are using process, people, and technology to improve vulnerability coordination and security investments in connecting vulnerability management to secure development. We understand that there is not a one-size-fits all approach to security. Every organization needs to regularly assess its process maturity and operational capacity to determine which security solutions make sense today and in the future.

  Luta Security advises organizations across all phases of vulnerability coordination, including smart roadmaps on how to comply with ISO standards 29147, 30111 and 27304. Our clients include the U.S. Department of Defense (DOD), the UK National Cyber Security Centre (NCSC), Facebook, and Zoom to name a few.

- **Team:** With over 30 years of combined professional security, technology, and government expertise, the Luta Security team is ready to guide your organization toward a more secure future. Leading the seasoned team is Luta Security CEO and Founder, Katie Moussouris.

  Katie is a computer hacker with more than 20 years of professional cybersecurity experience. She brings a unique and unparalleled perspective on security research, vulnerability disclosure, and bug bounties. She serves as a security advisor for several governments and large organizations around the world, and she is the co-author and co-editor of ISO standards in vulnerability disclosure (29147), vulnerability handling processes (30111), and secure development (27034).

- **Core Values:** Luta Security is guided by our core values of *respect, accountability, and pay equity*.

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

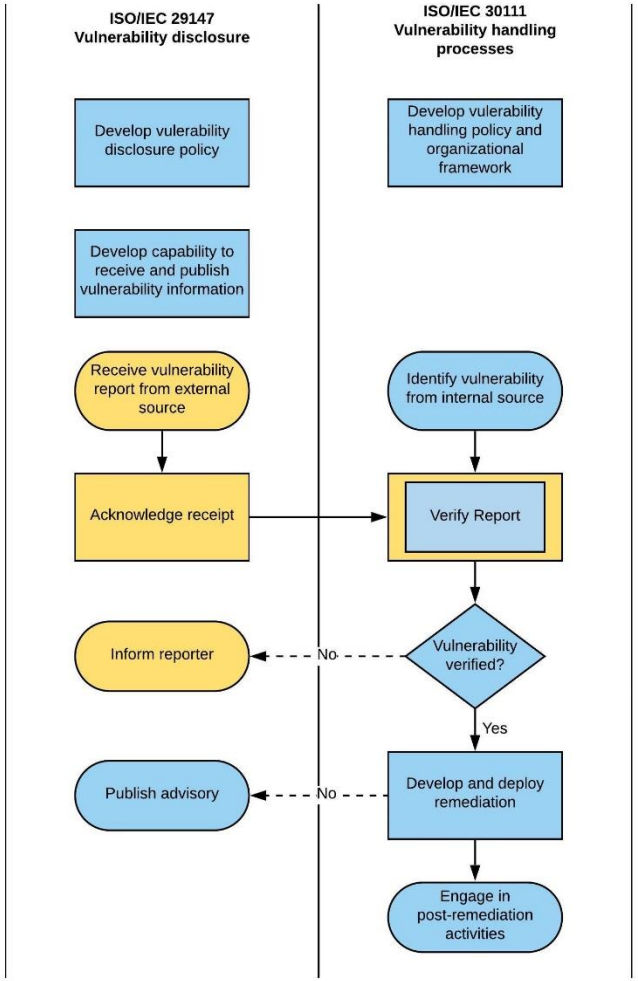
- Hackers for hire via a consulting arrangement
- Consultants have passed employment background checks
- **Contracts and NDAs make this a planned process**

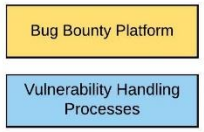
Bug Bounty Programs

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

88% of the Forbes Global 2000 have NO PUBLISHED WAY to report a security vulnerability.

ISO Standards 29147 & 30111





Not everyone is ready to implement ISO 29147, Vulnerability Disclosure

Everyone should be ensuring vulnerability handling compliance with ISO 30111 first

Scalable VDPs require planning, training, & resources

Commercial bug bounty platforms are not replacements for ISO 30111 or 29147

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?

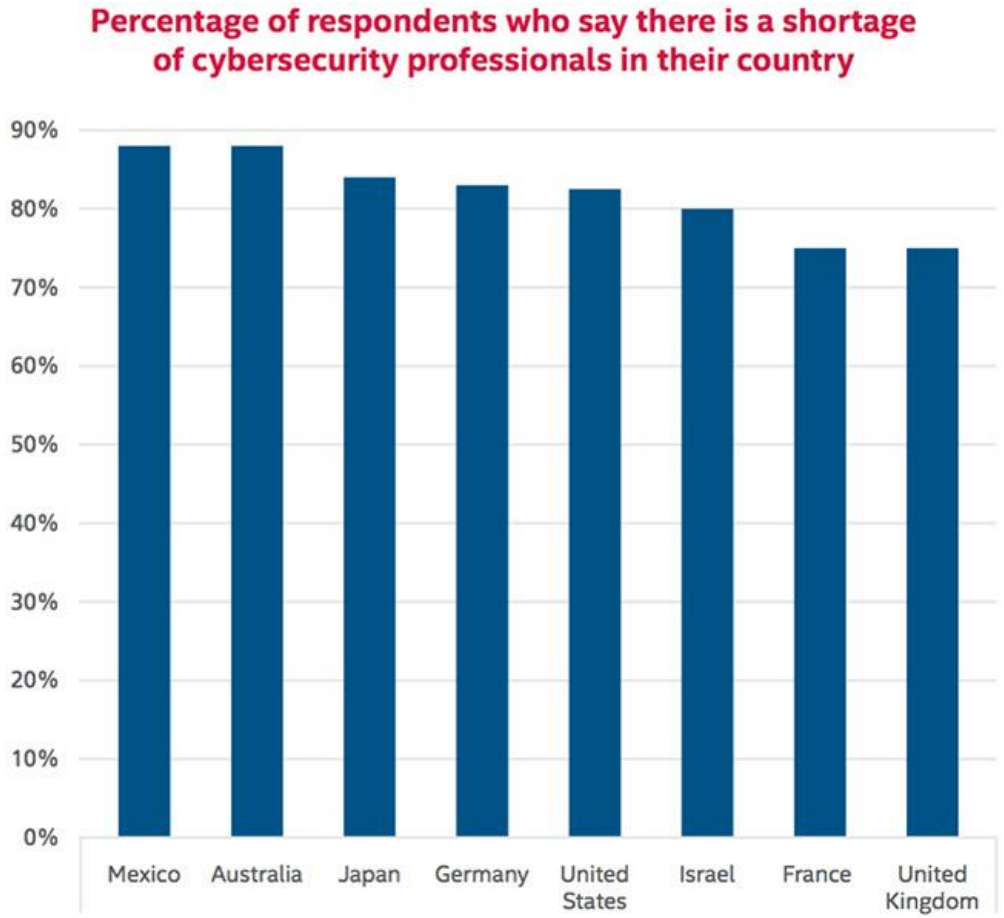
Isn’t This Problem Solved By Bug Bounty Platforms?

Manage the Flood, They Said

Only Validated Bugs, They Said

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

Cyber Workforce Shortage = Opportunity



82 percent of employers report a shortage of cybersecurity skills, and 71 percent believe this talent gap causes direct and measurable damage to their organizations.[1]

Unfilled cybersecurity jobs has grown by more than 50 percent since 2015.[3]

By 2022, the global cybersecurity workforce shortage is predicted to exceed 1.8 million unfilled positions.[4]

https://www.csis.org/analysis/cybersecurity-workforce-gap

https://www.helpnetsecurity.com/2016/07/28/cybersecurity-talent-crisis/

Triage Labor – The Job You'll Never Love

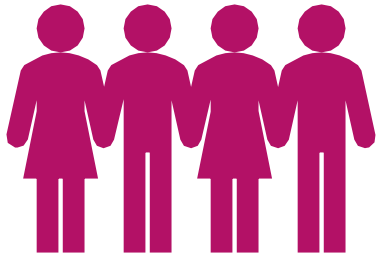
Microsoft receives between 150,000-200,000 non-spam email messages per year to secure@Microsoft .

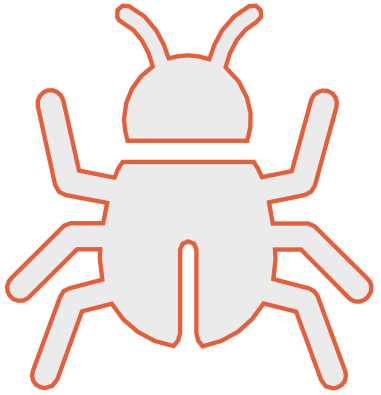
In 2007, Popular Science named "**Microsoft Security Grunt**" among the **Top 10 Worst Jobs in Science**.

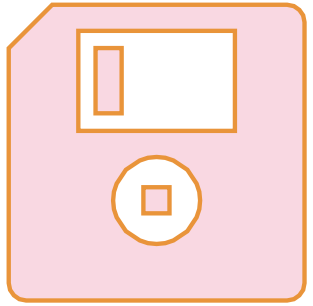
- This lands the triage/case management job between "**Whale Feces Researcher**" and "**Elephant Vasectomist**"
- This role is full-time, **pays six figures plus full benefits**, is held by several team members, & has the **highest turnover** of any job in the Microsoft Security Response Center

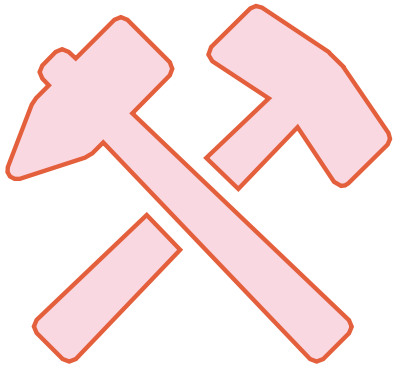
Labor Market for Bug Hunting vs Bug Fixing & Code Writing

- 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.
- **We are cranking out more bug writers than software developers & building a permanently indefensible ecosystem**

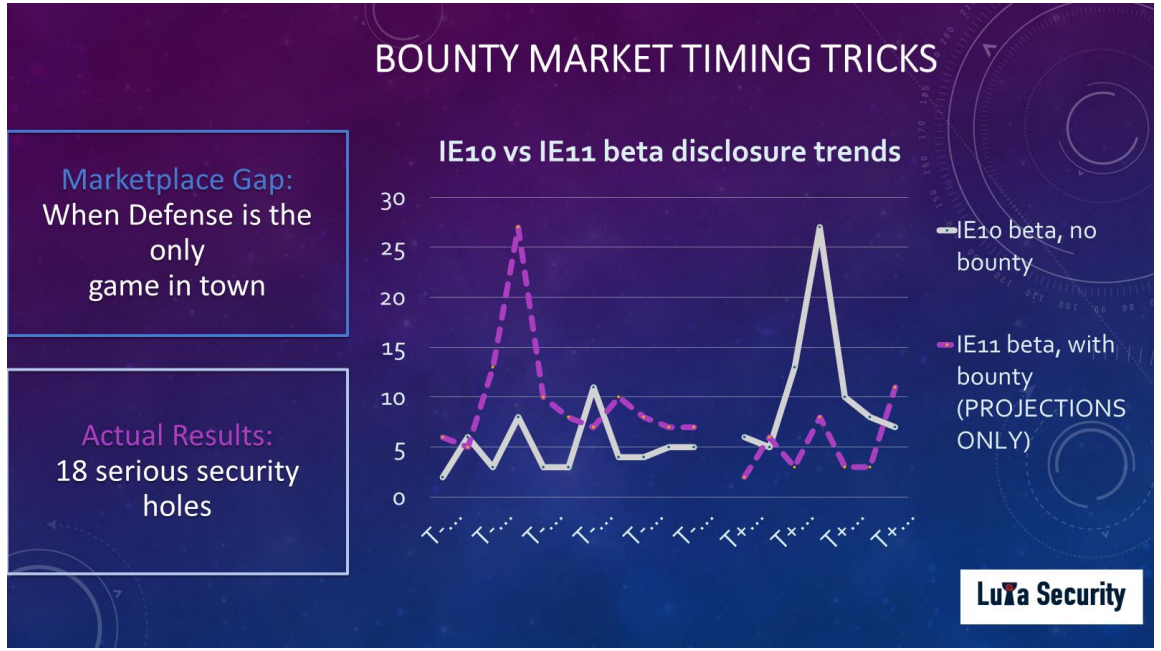


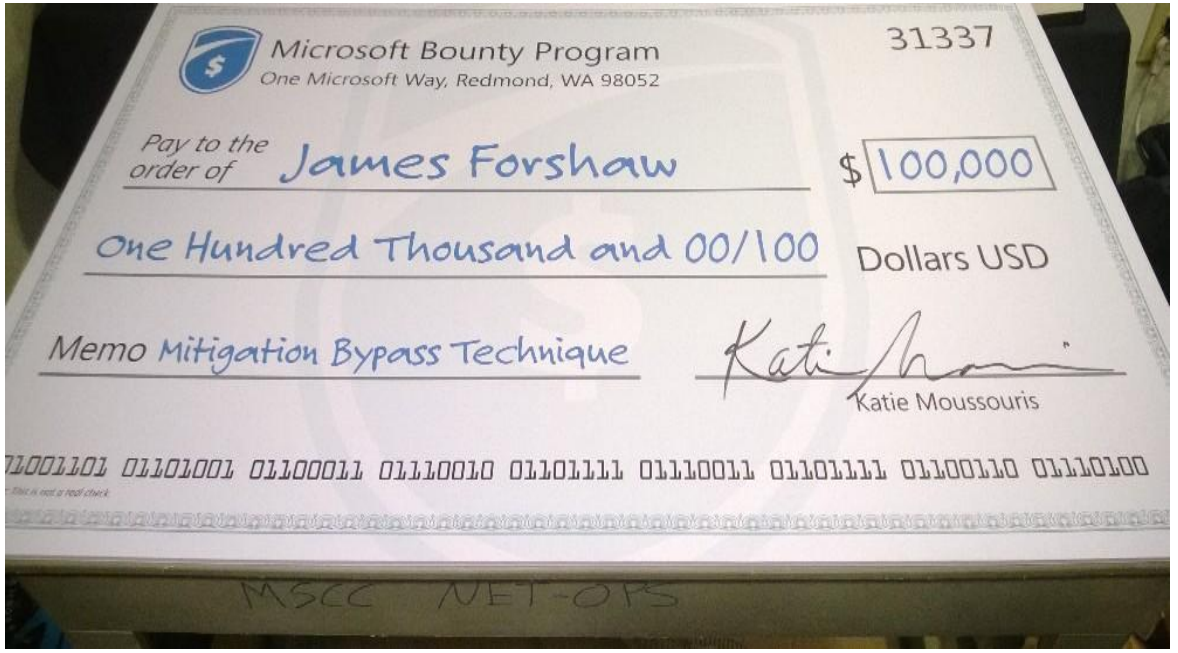






Microsoft Mutiny on the Bounty!





Bounty Smarter, Not Harder

Hack the Pentagon – Hack the Planet!

BY THE NUMBERS

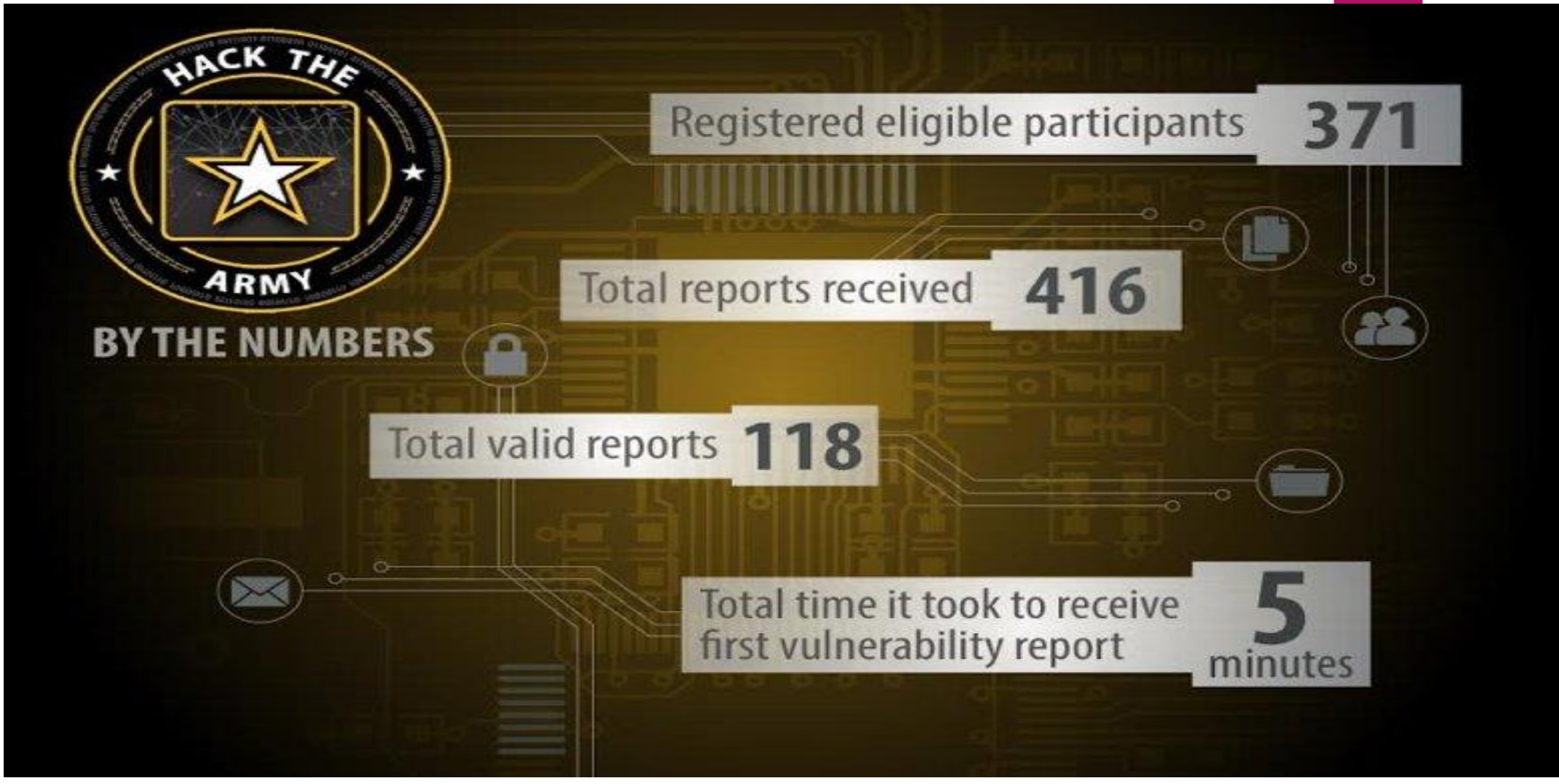
Registered eligible participants **1,410**

Total reports received **1,189**

Total valid reports **138**

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

Hack The Army – Gently With a Chainsaw



Gaps in the BOD Guidance

- While **CISA should be commended** for getting some guidance out to agencies, the initial steps are out of order, leaving significant capability and key preparation gaps.
- To ensure success, the U.S. government should have provided initial guidance on how to comply with all the relevant ISO standards before issuing a BOD on VDPs.
- To that point, the public announcement of a VDP and its operation as described in ISO 29147 should only come after an agency has a measurable vulnerability handling process as described in ISO 30111.
- If agencies engage in a VDP before internal handling processes are fully in place, understood and resourced, there are risks including missing key reports, or frustrating the researcher community, and **making systems even less safe**.

Keep Building Internal Capabilities

- The NIST report *The Economic Impacts of Inadequate Infrastructure for Software Testing* from 2002 analyzes the cost benefits of finding bugs earlier in the development process.
- Disclosure without mature handling processes are like a door to nowhere
- **Up to 45x more costly to remediate vulnerabilities at the VDP/Bug Bounty Stage**

4.1.2 Detecting Bugs Sooner

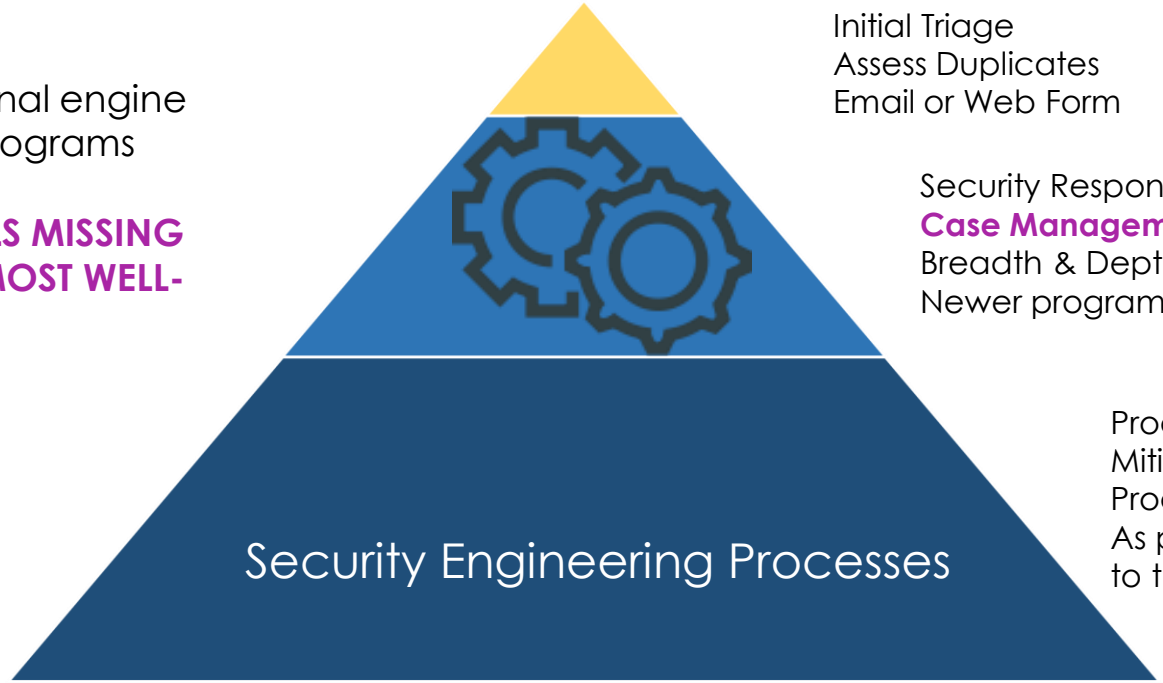
"Test early, test often" is the mantra of experienced programmers. When defects are detected early in the software development process, before they are allowed to migrate to the next stage, fewer remain in the shipped product and they are less costly to correct than if they are discovered later in the process (Kit, 1995).

The Economic Impacts of Inadequate Infrastructure for Software Testing, NIST, 2002

Best Practices: Resource Allocation for VDPs

The 2nd layer is the operational engine of Vulnerability Disclosure Programs

KEY PEOPLE, PROCESS, TOOLS MISSING IN MOST ORGS - EVEN THE MOST WELL-RESOURCED



Initial Triage
Assess Duplicates
Email or Web Form

Security Response Center / Product Security
Case Management – Researcher interface
Breadth & Depth Analysis
Newer programs- the majority of work focused here

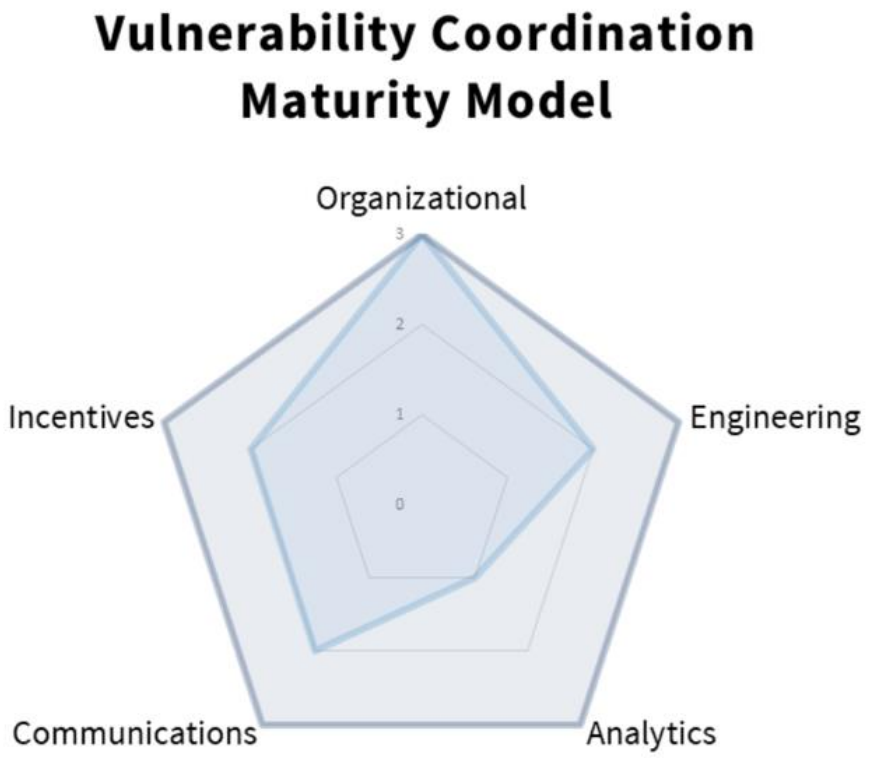
Product Engineering
Mitigation Strategy
Product roadmap evaluation
As programs mature- the majority of work shifts to this layer

VDPs accelerate the need to improve internal security engineering, secure development, and internal case management infrastructure

Maturity Assessments -VCMM

To improve overall security, every organization needs to benchmark its capabilities and identify and prioritize areas that need improvement.

The Vulnerability Coordination Maturity Model (VCMM) provides a framework that evaluates five key areas to help organizations measure and evolve their vulnerability management capabilities.



www.lutasecurity/vcmm

#NotAllBugs Are Created (or Fixed) Equally

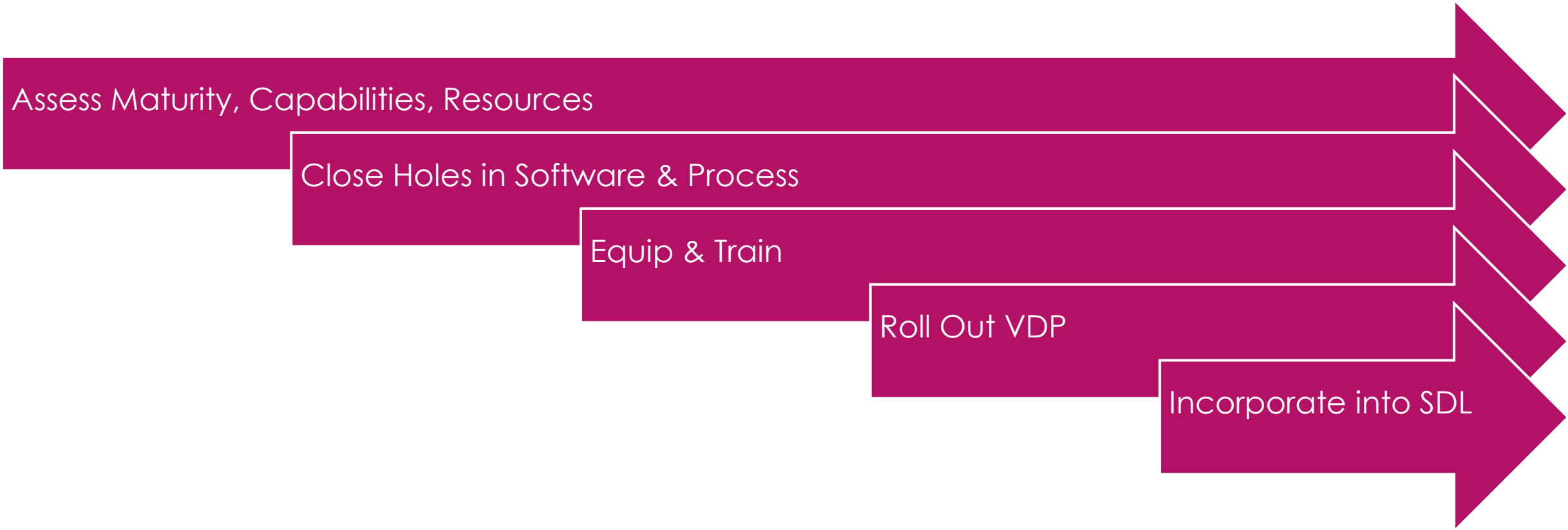
Creating a Vulnerability Typology

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

Recommendations

- Complete a maturity assessment for all 5 areas of the VCMM
- Using the assessment, set realistic goals and priorities for maturing the security of your organization
- Create a roadmap for **building compliance with ISO 30111 BEFORE attempting 29147**
  - Determine necessary budget
  - Hire where necessary & train internal personnel
  - Measure both **response speeds and bug complexity** to gauge progress & improve people process and tech
- Release data transparently in an annual report

Recommended Order Of Operations



Recommend VDP 2 Years Minimum Before Bug Bounties

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

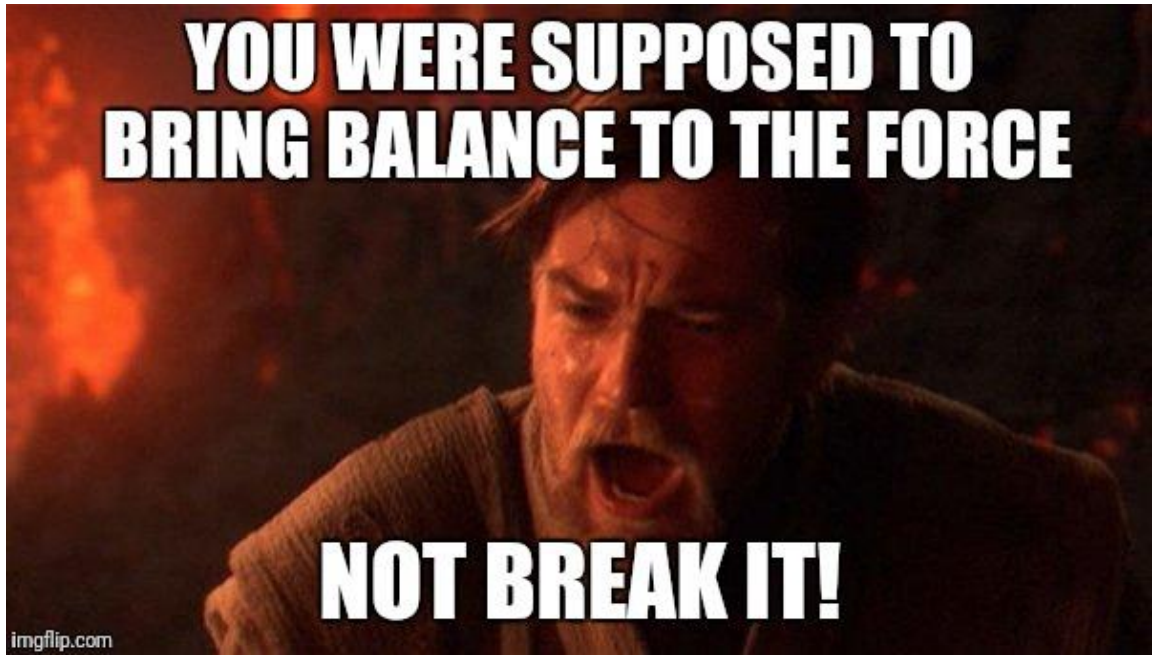
Capacity Planning & Maturity is the Right Way Forward

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

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

Balance The Labor Workforce



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

Luta Security

info@lutasecurity.com

KATIE MOUSSOURIS, CE0 & FOUNDER, LUTA SECURITY

@K8EM0