



Security is a Neverending Story

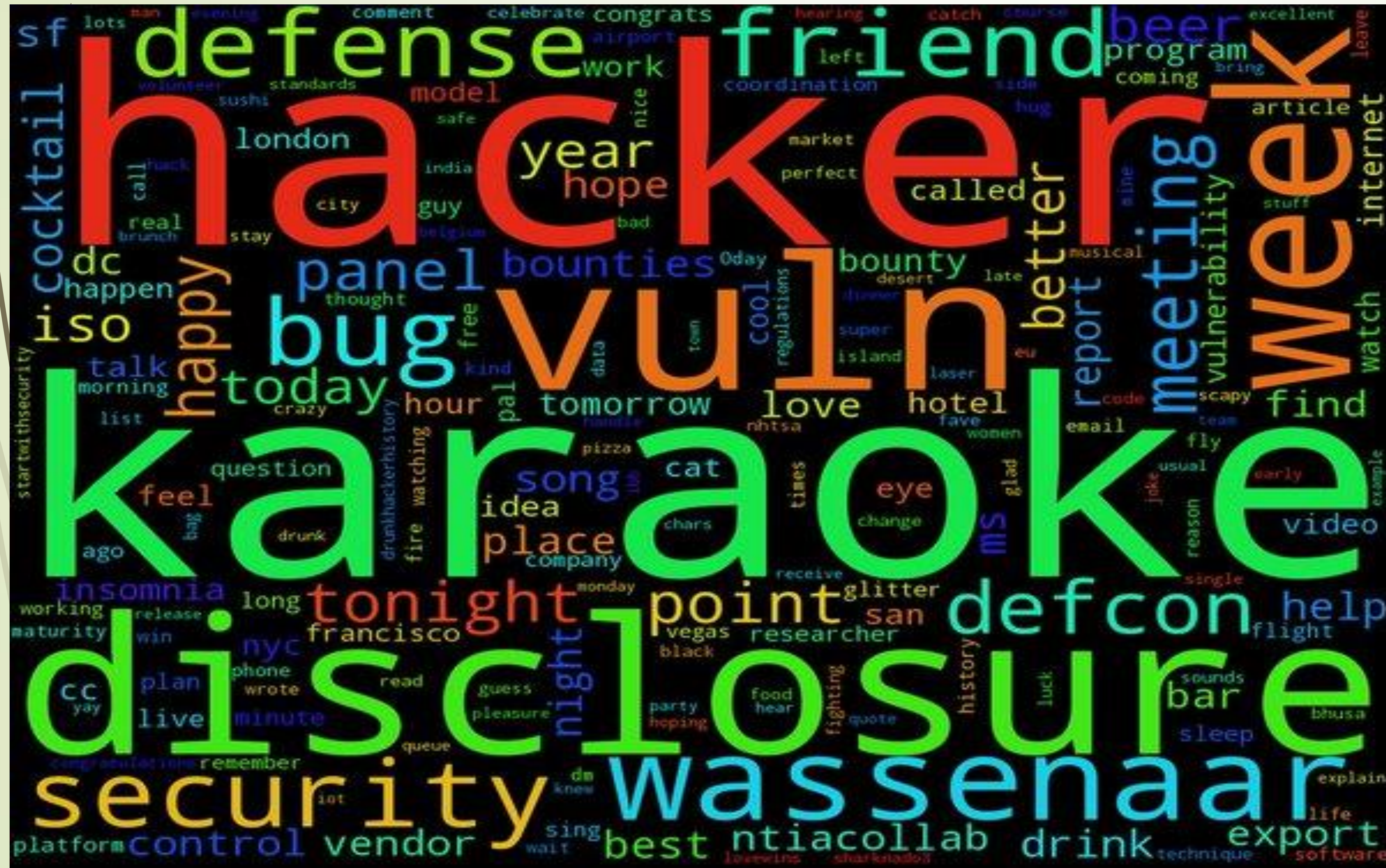
CEO Luta Security Inc
@lutasecurity @k8em0

Katie Moussouris

We're Going to Need More than Luck



Who the F\$CK Are You? What is it you do here?



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



Every Story Has A
Beginning

Hacker for Hire – Learning Empathy



Don't Let the Rain Get You Down

ALL

CODE

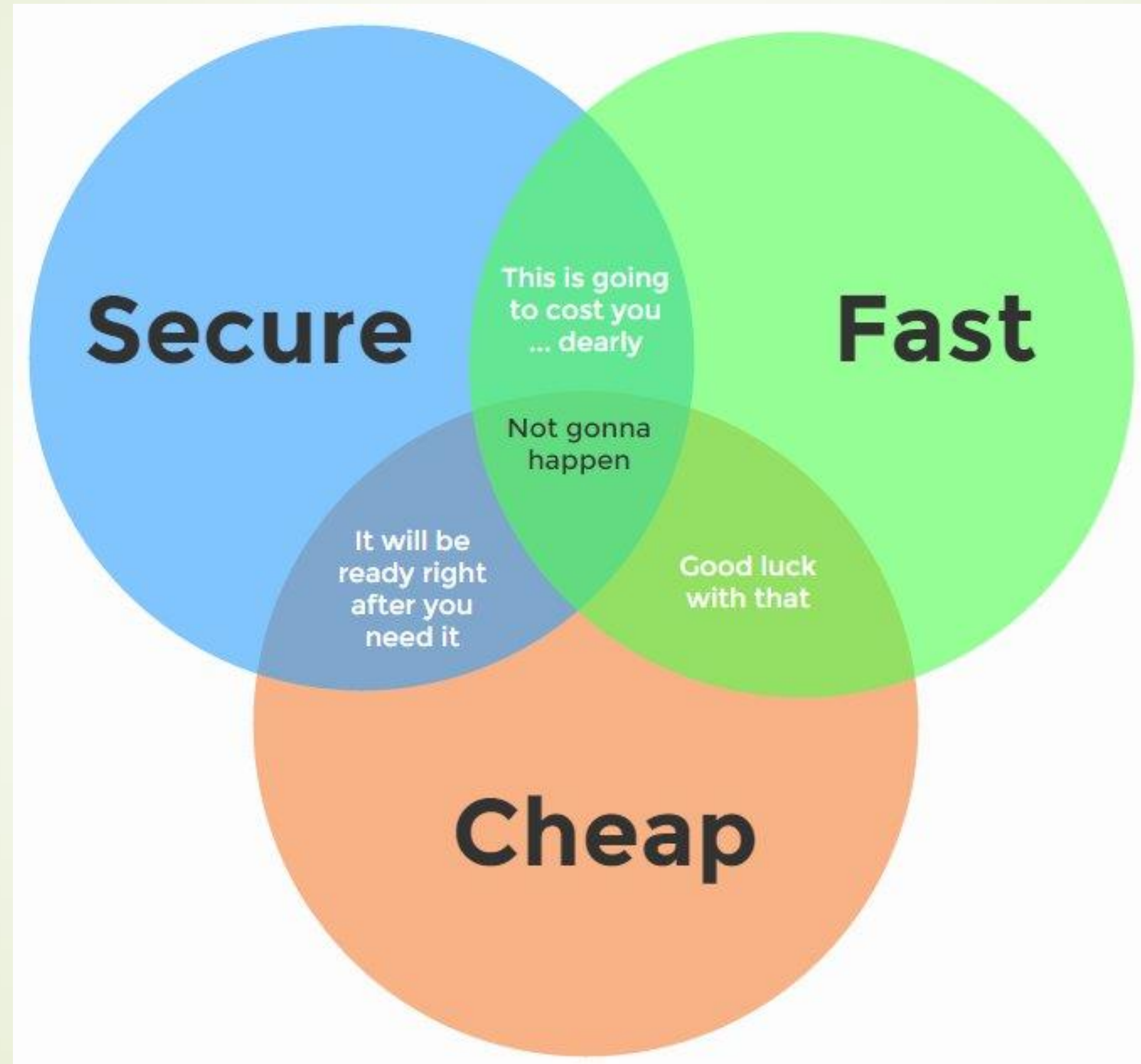
HAS

SECURITY

BUGS



This Guy is Onto Something



Thanks <https://twitter.com/virturity/status/799242892082429953>


I' m a Hacker and I' m Here to Help



@lutasecurity

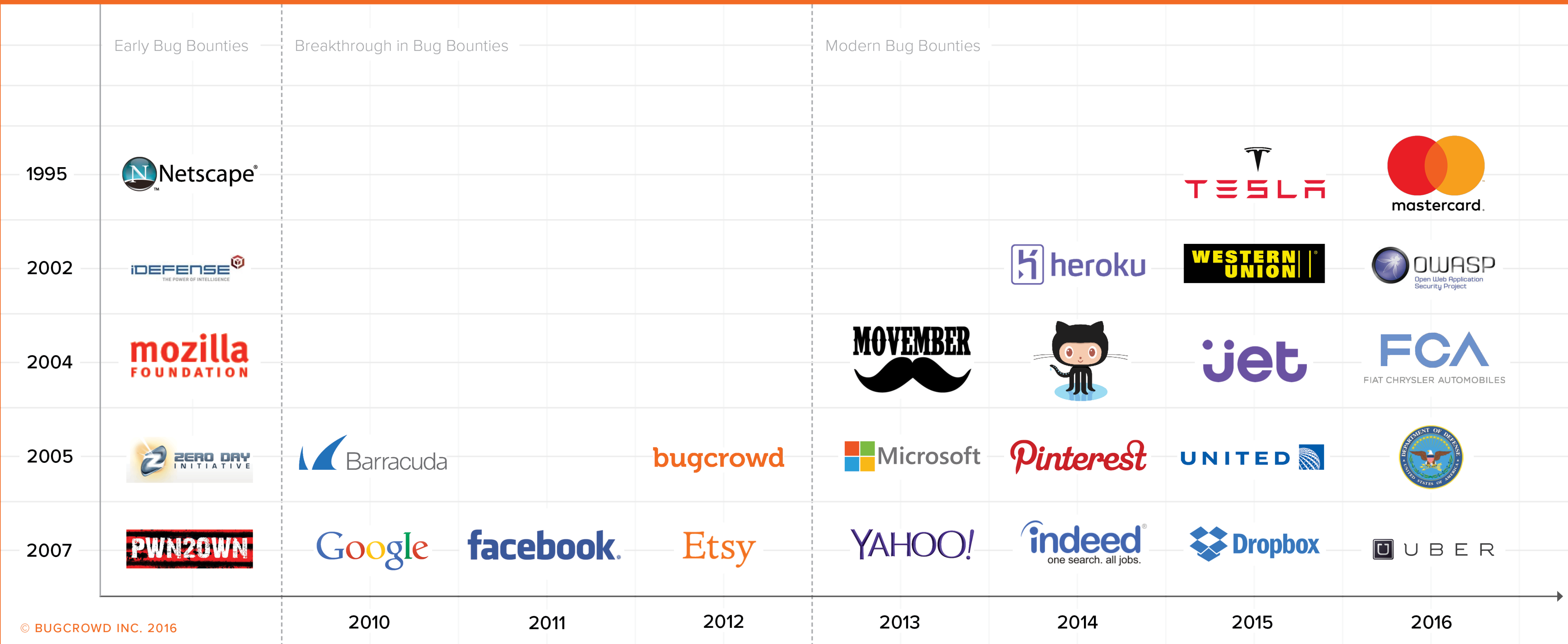
@k8em0

LuKa Security



History of Vulnerability Disclosure and Bug Bounty Programs

The History of Bug Bounties: Abbreviated Timeline from 1995 to Present



© BUGCROWD INC. 2016


Vulnerability Disclosure vs. Bug Bounty Programs

- **Vulnerability Disclosure**

- Ensures that organizations are ready to handle vulnerability reports.
- Follows the ISO standards for vulnerability disclosure (ISO 29147) and vulnerability handling processes (ISO 30111).
- **94% of the Forbes 2000 companies don't have this in place**

- **Bug Bounty Programs**

- Some organizations and governments choose to offer cash rewards for bugs.
- Some do it alone (e.g. Microsoft), while the majority choose a bug bounty service provider to help.
- **Bug Bounties can work in large and small organizations, with some prep & help**



Bug Bounty
vs
Penetration
Testing
And Bug Bounty
Service Providers

Differences from standard testing



Single-sourced

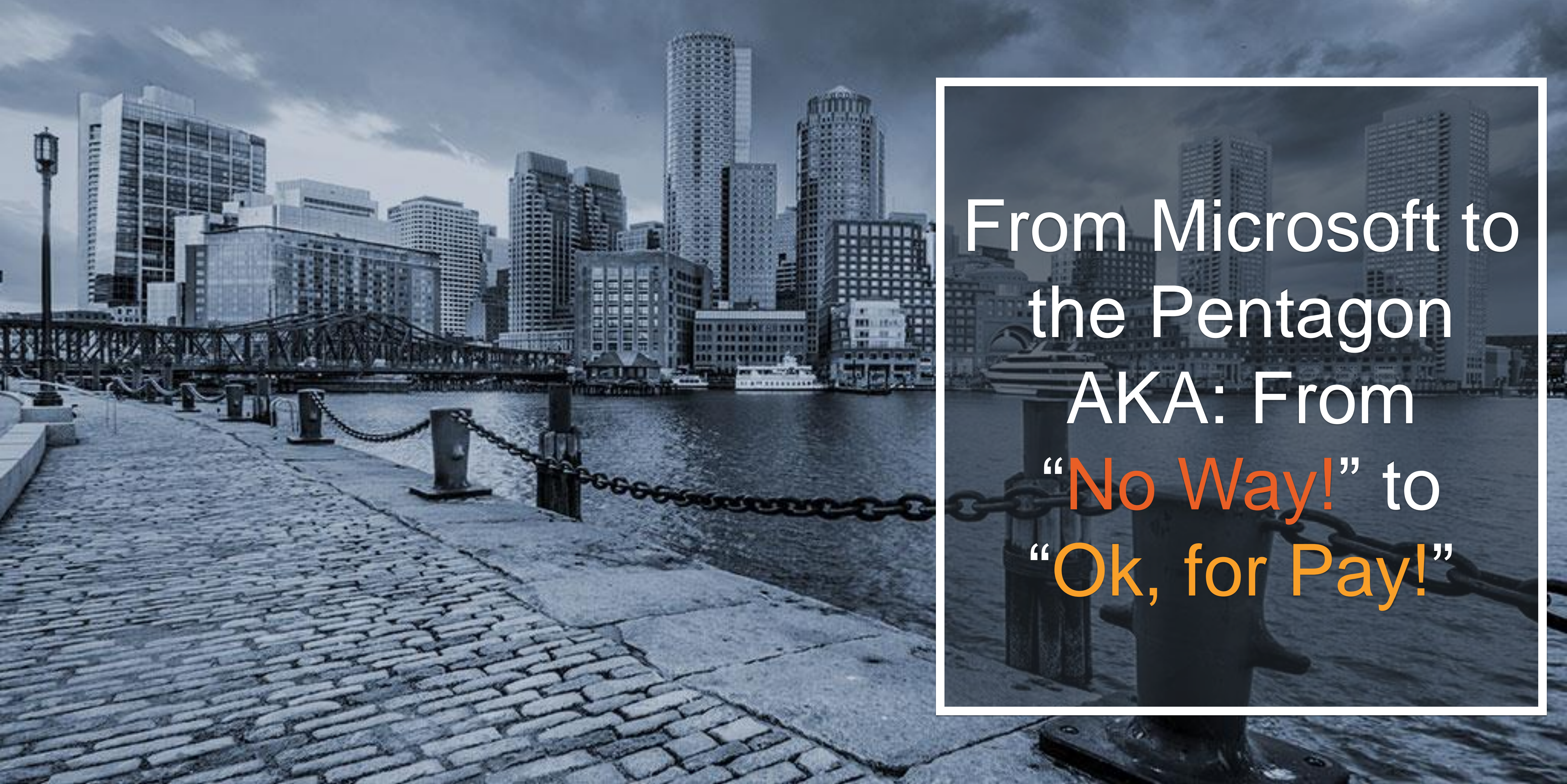
- looking mostly for common-ish vulns
- not competing with others
- incentivized for count
- payment based on sniff test

Crowdsourced

- looking for vulns that aren't as easy to find
- racing vs. time
- competitive vs. others
- incentivized to find unique bugs
- payment based on impact not number of findings

Bug Bounty Service Providers – At a glance

BugCrowd	HackerOne	Synack
The Easy Button for Triage	Platform for Power Users	Secret Squirrels
Great if you need triage support, less so if you don't want triage outside your company's eyes only	Great if you want automation for your own vulnerability handling, less so if you lack the internal talent to use it	Great if you want a crowd-sourced penetration test under NDA, less so if you need a broader pool of eyes



From Microsoft to
the Pentagon
AKA: From
“No Way!” to
“Ok, for Pay!”

Microsoft Security Response Center

Microsoft Security Response Center (MSRC) works with security researchers around the world to help prevent security issues and to advance Microsoft product security.



New Mitigation Bypass Techniques
\$100,000
Bounty Evolution

Recycle



Security Researcher Engagement



Industry Collaboration



Security Response Center investigates all security vulnerabilities in Microsoft products and services.

The Bluehat team supports collaboration and relationships with security researchers globally to advance Microsoft product security.

Microsoft supports collaboration across the security community so that customers can take timely action to reduce their customer's while minimizing risk to the ecosystem.

Microsoft's Strategic Bounty Programs:



\$100,000 for new techniques



\$50,000 for new defenses



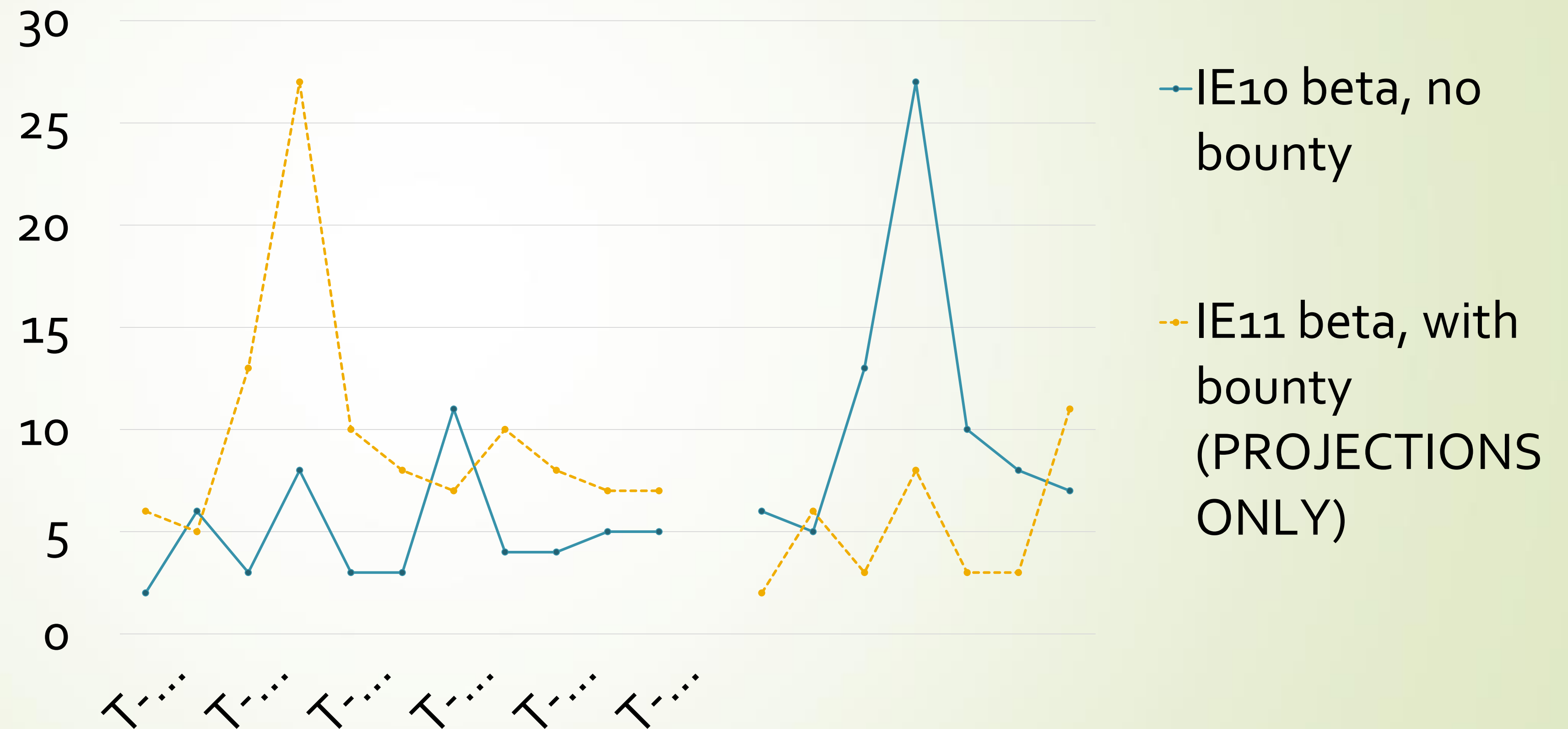
\$11,000 for IE11 beta bugs

Bounty Market Timing Tricks

Marketplace Gap:
When Defense is the
only
game in town

Actual Results:
18 serious security
holes

IE10 vs IE11 beta disclosure trends



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!



Coming in 2017: A Wave of Bug Bounties



Avoid these pitfalls, in Planning Bounties & Marathons

“Failing to plan is planning to fail.”

“Don’ t reinvent the wheel, just realign it.”

Rushing into a bug bounty without preparation is like running a marathon immediately following a coma.

You’ re not a snowflake. Except that you are. Except that you’ re not when it comes to vulnerability disclosure.





With Great
Regulation Comes
Great
Responsibility



Swinging from the Cyberlier



Policy: I Do Not Think It Means What You Think It Means



- Not pronounced “police-y”
- I’m not a lobbyist, not a lawyer, though the activities are related
- I help advise lawmakers, regulators, governments

* Photo credit Dave Aitel

Wassenaar? Gesundheit!

- 41 countries trying to control weapons proliferation
- December 2013: Added “intrusion software” and “intrusion software technology” to the list of controlled weapons
- May 2015: US proposed a draft implementation of the export control rule to comply with Wassenaar



ALL HELL BREAKS LOOSE!

INTENT vs RESULT:

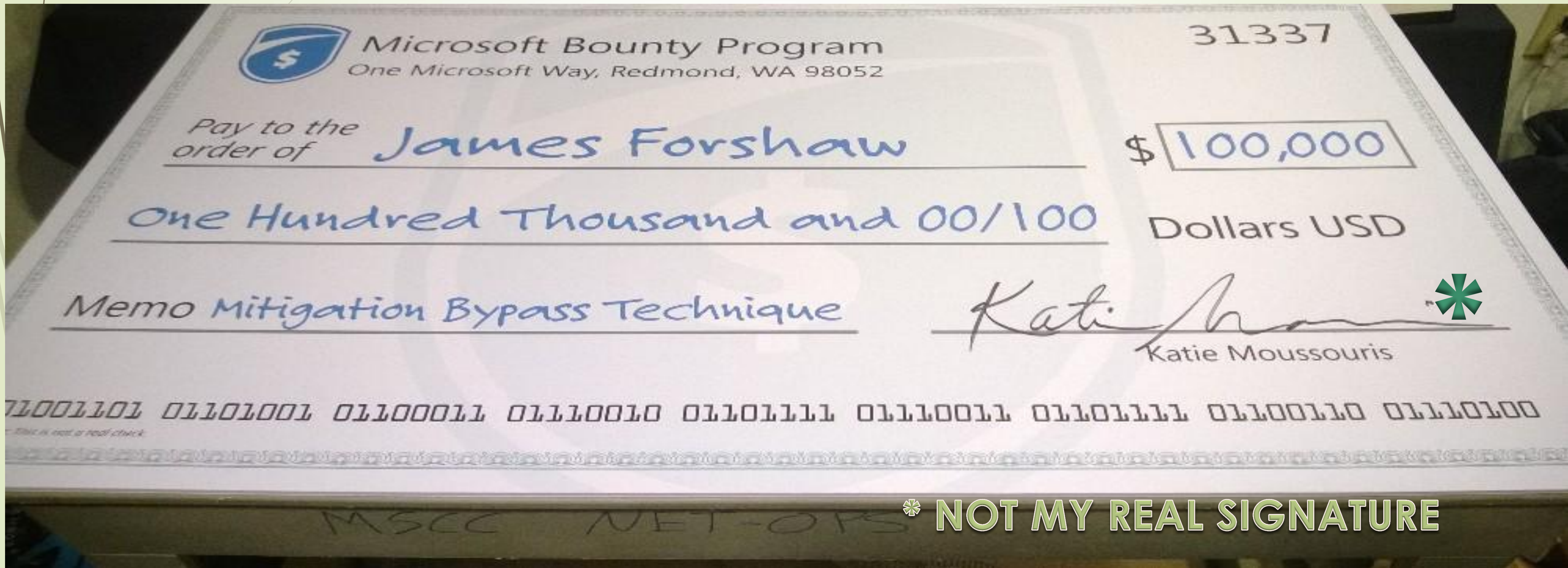
- Meant to regulate surveillance software, keeping it from being sold to repressive regimes who would use it to abuse human rights (Sudan, Syria, etc)
- Ends up catching all kinds of software and technology that is useful for defense

BREAKS THE ABILITY FOR THE INTERNET TO DEFEND ITSELF



MITIGATION BYPASS BOUNTY: \$100,000 for a Technique

James and the Giant Check



Finger on (or near) The Button





Seems
Easy,
Right?





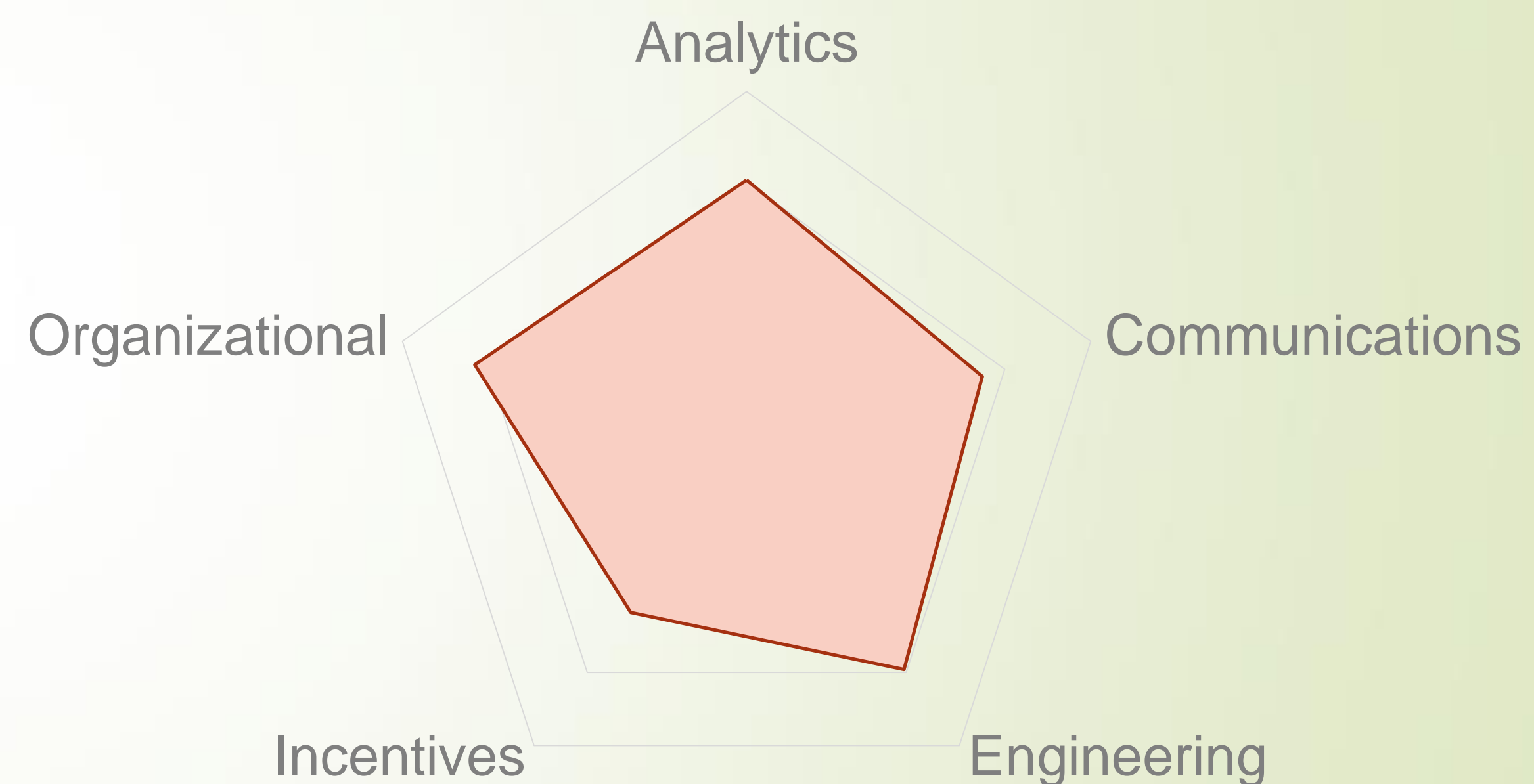
Vulnerability
Coordination
Maturity Model

Where to begin

Where to go

Vulnerability Coordination Maturity Model

- Model guides how to organize and improve vulnerability disclosure processes
- 5 Capability Areas: Organizational, Engineering, Communications, Analytics and Incentives
- 3 Maturity Levels for each Capability: Basic, Advanced or Expert
- Organizations can benchmark their capabilities



Organizational



Organizational

People, process, and resources to handle potential vulnerabilities

Level --Capability

Basic

Executive support to respond to vulnerability reports and a commitment to security and quality as core organizational values.

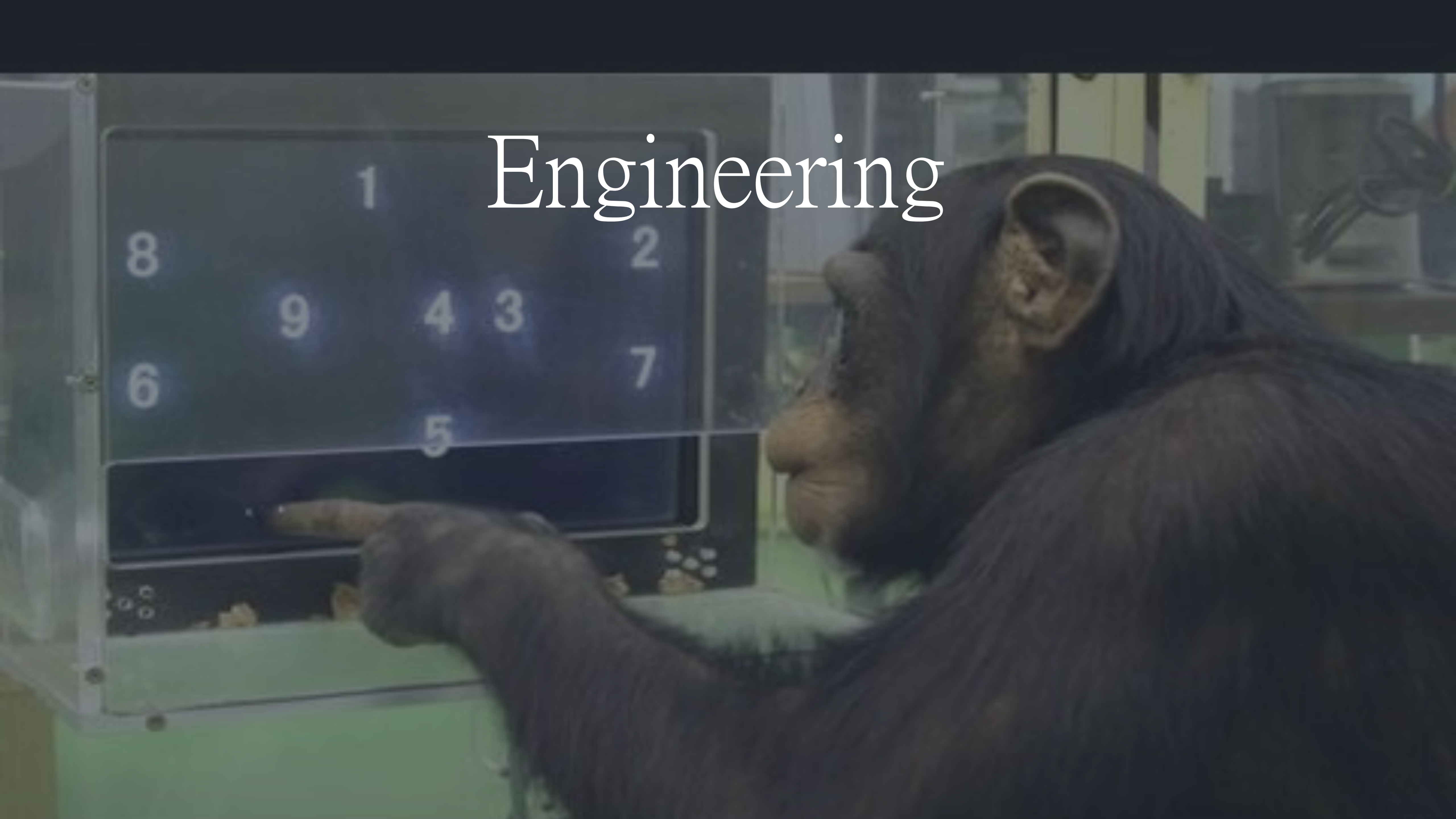
Advanced

Policy and process for addressing vulnerabilities according to ISO 29147 and ISO 30111, or a comparable framework.

Expert

You have executive support, processes, budget and dedicated personnel for handling vulnerability reports.

Engineering



Engineering:

Capabilities to evaluate and remediate security holes, and improve software development lifecycle

Level -- Capability

Basic

Clear way to receive vulnerability reports, and an internal bug database to track them to resolution. See ISO 29147.

Advanced

Dedicated security bug tracking and documentation of security decisions, deferrals, and trade-offs.

Expert

Use vulnerability trends and root cause analysis to eliminate entire classes of vulnerabilities. See ISOs 29147, 30111, 27034.

Communication



Communications

Ability to communicate to audiences internally and externally about vulnerabilities.

Level - Capability

Basic

Ability to receive vulnerability reports and a verifiable channel to distribute advisories to affected parties. See ISO 29147.

Advanced

Tailored, repeatable communications for each audience, including security researchers, partners, customers, and media.

Expert

Structured information sharing programs with coordinated distribution of remediation.

Analytics



Analytics

Data analysis of vulnerabilities to identify trends and improve processes.

Level - Capability

Basic

Track the number and severity of vulnerabilities over time to measure improvements in code quality.

Advanced

Use root causes analysis to feed back into your software development lifecycle. See ISOs 29147, 30111, 27034.

Expert

Track real-time telemetry of active exploitation to drive dynamic pivots of remediation strategy.



Incentives

Incentives

Ability to encourage security researchers to report vulnerabilities directly.

Level - Capability

Basic

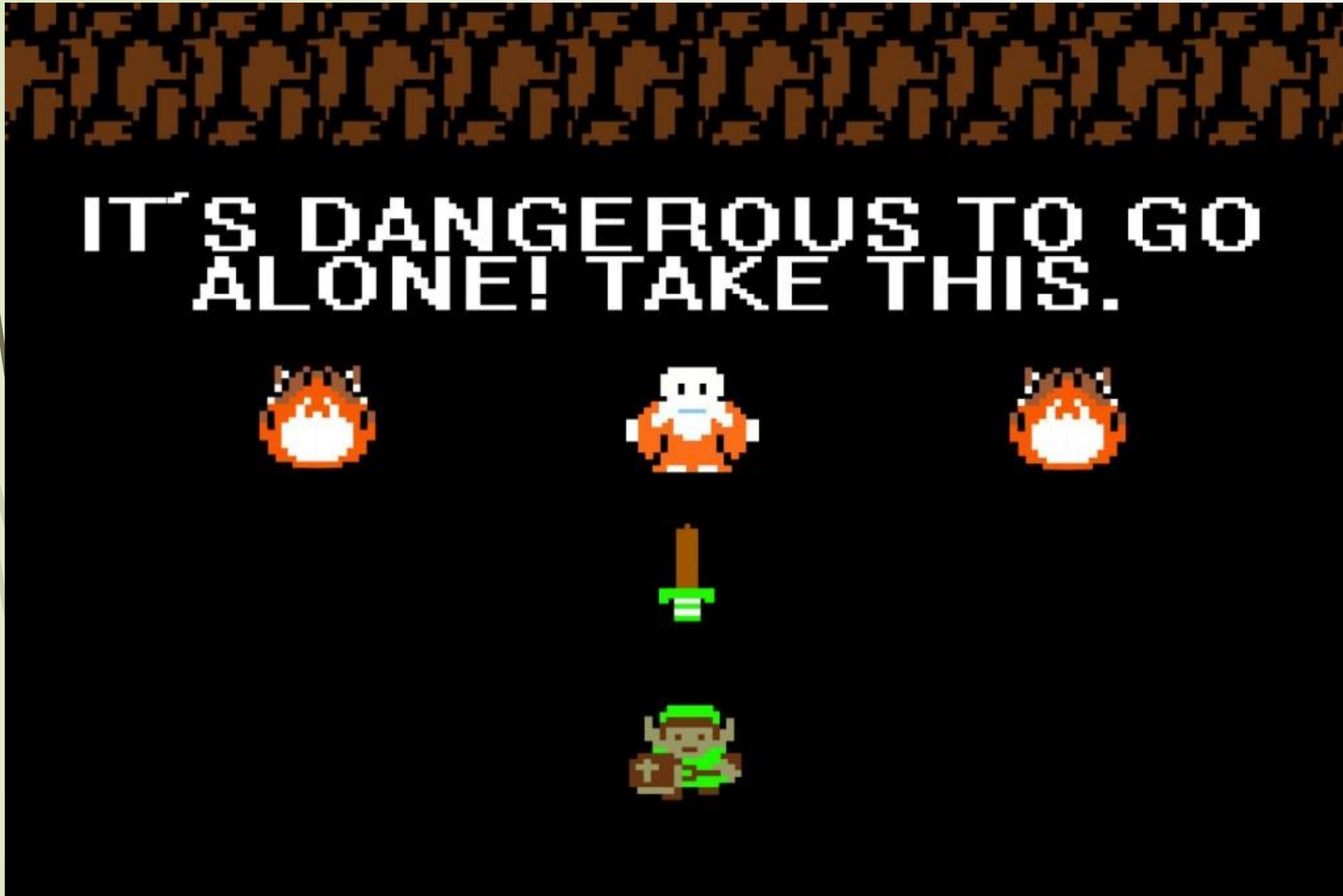
Show thanks or give swag. Clearly state that no legal action will be taken against researchers who report bugs.

Advanced

Give financial rewards or bug bounties to encourage reporting the most serious vulnerabilities.

Expert

Understand adversary behavior and vulnerability markets, and structure advanced incentives to disrupt them.



Someone Will
Disclose a Bug
to You
or breach you.

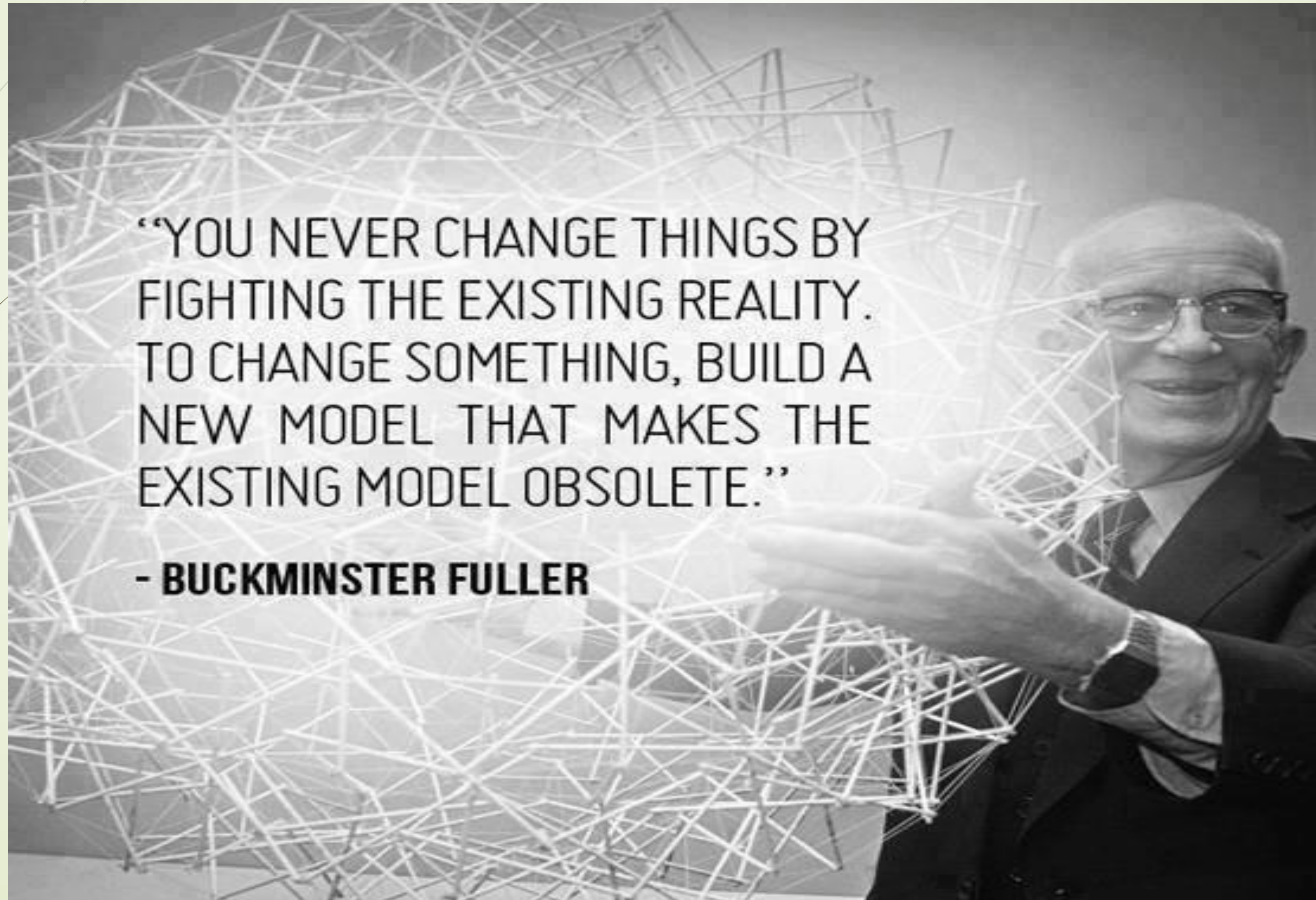
Not if. When.

Proactive Steps

1. Take the **Vulnerability Coordination Maturity Model** Assessment today to assess your capabilities
2. **Ask for help** from those who have come before to develop your strategic and tactical plan for the inevitable vulnerability report
3. **Consider your goals** if seeking a bug bounty or any other security service provider
4. **Vulnerability Disclosure is among your first steps**, master that, and practice the EMPATHY that security requires.
5. **Build Security In** whenever you can, but know that **you will not be able to catch everything**

Bug Bounties don't need to spill **blood** in the water.
Bug Bounties won't replace other security testing.
Hackers can help you – if you let them!

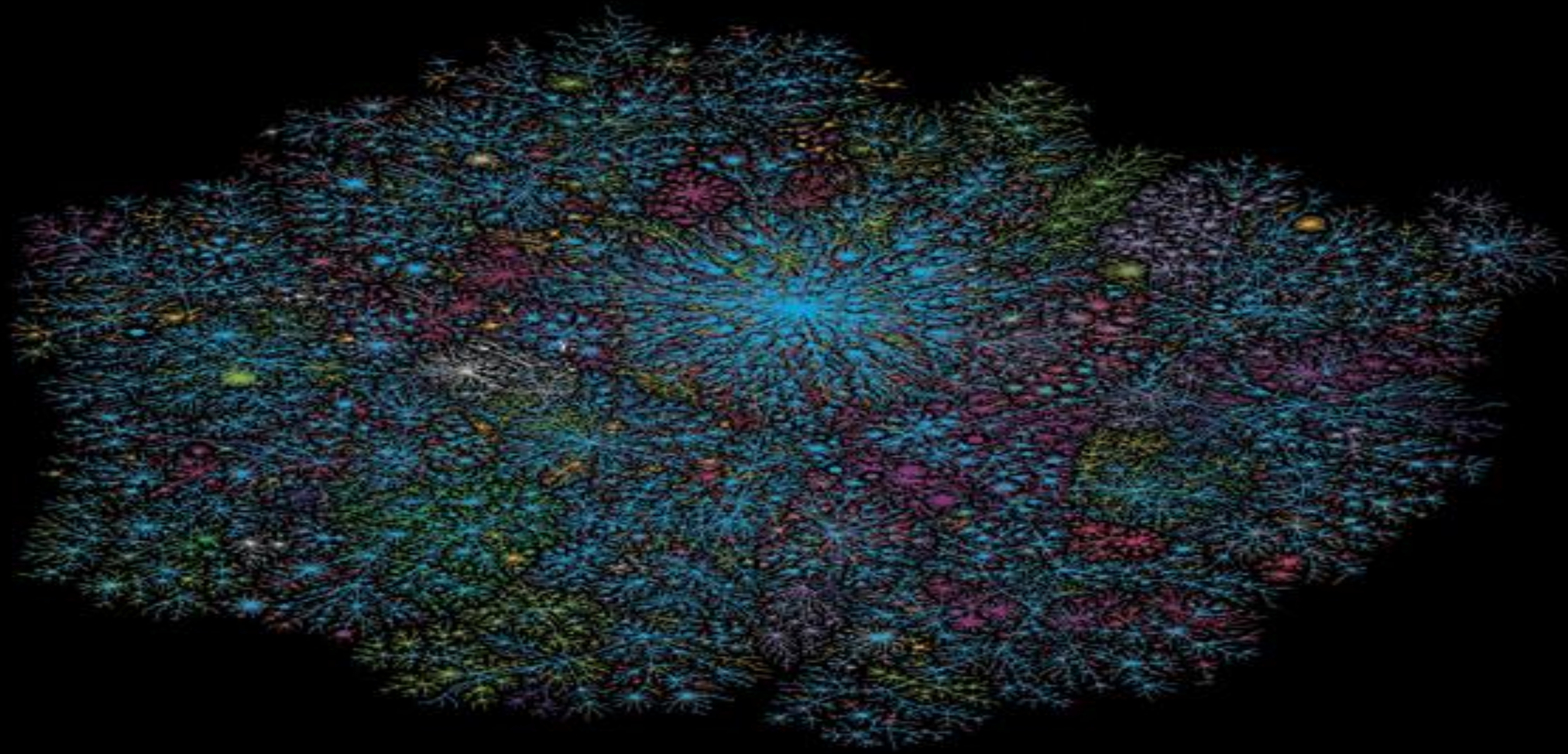
Change is the only constant → **EVOLVE**



“YOU NEVER CHANGE THINGS BY FIGHTING THE EXISTING REALITY. TO CHANGE SOMETHING, BUILD A NEW MODEL THAT MAKES THE EXISTING MODEL OBSOLETE.”

- **BUCKMINSTER FULLER**

THE WHOLE INTERNET



North America Central America South America Africa South Africa Europe Germany France Netherlands United Kingdom Asia India Pacific Islands Australia New Zealand Asia East Asia Asia Southeast Asia Asia South Asia Asia West Asia

The shape of the network was created by plotting the network and coloring it according to the geographic location of the nodes. The size of the nodes is proportional to the number of connections they have. The size of the lines is proportional to the number of connections between nodes.

Source: Internet Map by Washington, D.C. (http://www.internetmap.com) and the Internet Map Project (http://www.internetmap.com/). The map data is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike license.

This map was created using the same data as the map above, but with the nodes colored by the number of connections they have. The size of the nodes is proportional to the number of connections they have.

Where Will Your Security Story Take You?

