RSA®Conference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **KEY-F01S**

Coordinated Vulnerability Disclosure: You’ve Come a Long Way, Baby

Katie Moussouris

Founder & CEO
Luta Security
@k8em0

Chris Wysopal

Co-founder @ CTO
Veracode
@WeldPond

#RSAC

Non-Interchangeable Vuln Discovery Words Matter

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!**

Survey on Coordinated Disclosure

- Conducted by 451 Research from December 2018 to January 2019
- 1,000 respondents across a range of industries and organization sizes in the US, Germany, France, Italy and the UK.
- Respondents reported enterprise roles such as application development, infrastructure and information security, as well as security consultants, third-party vulnerability assessors or penetration testers, and independent security researchers.
- Respondents were required to have an average to high level of familiarity with vulnerability disclosure models to participate.
- **https://info.veracode.com/survey-report-451-research-exploring-coordinated-disclosure.html**

First let’s start with some history…

L0pht gets an email from Microsoft

Nov, 1997 Dildog@l0pht.com releases IE 4.0 RCE vulnerability and POC without coordinating with the vendor.

A week later Scott Culp from MSRC contacts contact@l0pht.com.

A haiku:

Microsoft IE
Is there no security?
Not if you ask me.

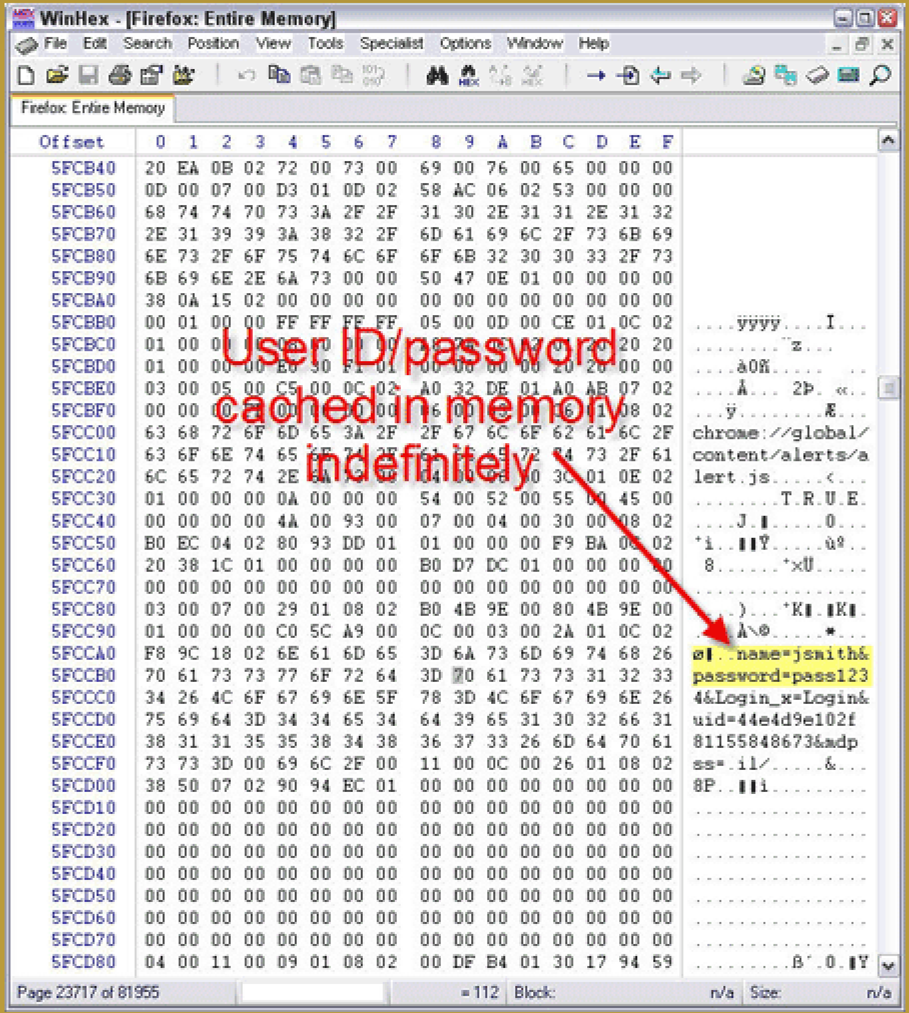
dildog@l0pht.com
(11/1/97)

MSRC First Contact with the l0pht vs Rain Forest Puppy

1999: RFPolicy attempted to codify expectations for disclosure.

No more open-ended forever-days?

The Lexar “JumpDrive Secure” CVD Gone Cattywampus

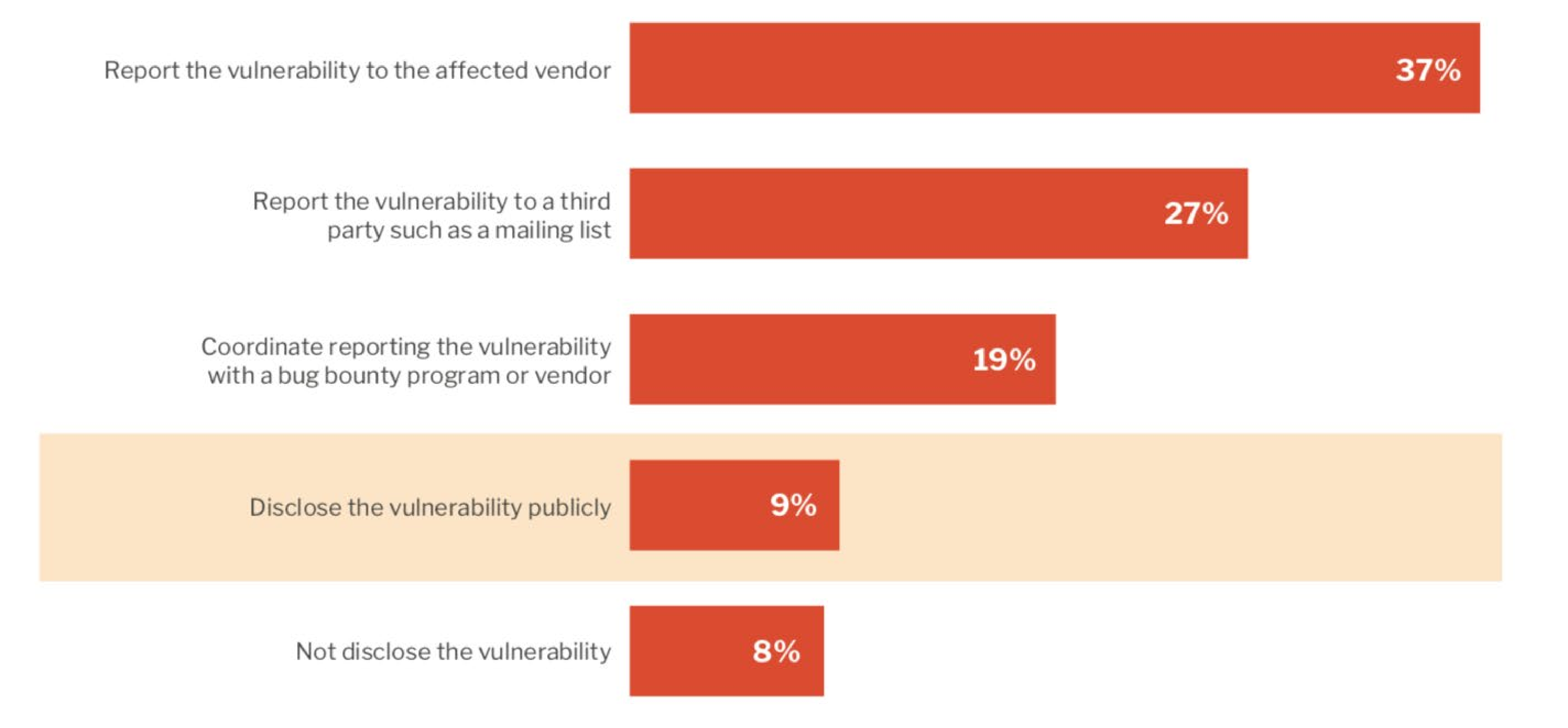

WinHex - [Firefox: Entire Memory]
File Edit Search Position View Tools Specialist Options Window Help
Firefox: Entire Memory

```
Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
5FCB40   20 EA 0B 02 72 00 73 00  69 00 76 00 65 00 00 00
5FCB50   0D 00 07 00 D3 01 0D 02  58 AC 06 02 53 00 00 00
5FCB60   68 74 74 70 73 3A 2F 2F  31 30 2E 31 31 2E 31 32
5FCB70   2E 31 39 39 3A 38 32 2F  6D 61 69 6C 2F 73 6B 69
5FCB80   6E 73 2F 6F 75 74 6C 6F  6F 6B 32 30 30 33 2F 73
5FCB90   6B 69 6E 2E 6A 73 00 00  50 47 0E 01 00 00 00 00
5FCBA0   38 0A 15 02 00 00 00 00  00 00 00 00 00 00 00 00
5FCBB0   00 01 00 00 FF FF FF FF  05 00 0D 00 CE 01 0C 02   ....ÿÿÿÿ....Î...
5FCBC0   01 00 [illegible]                          20 20   ..........¨z...
5FCBD0   01 00 00 00 E0 30 F1 01  00 00 00 00 20 20 00 00   ....à0ñ.....  ..
5FCBE0   03 00 05 00 C5 00 0C 02  A0 32 DE 01 A0 AB 07 02   ....Å... 2Þ. «..
5FCBF0   00 00 [illegible]                          08 02   ...ÿ.........Æ...
5FCC00   63 68 72 6F 6D 65 3A 2F  2F 67 6C 6F 62 61 6C 2F   chrome://global/
5FCC10   63 6F 6E 74 65 [illegible]           84 73 2F 61   content/alerts/a
5FCC20   6C 65 72 74 2E [illegible]           3C 01 0E 02   lert.js.....<...
5FCC30   01 00 00 00 0A 00 00 00  54 00 52 00 55 00 45 00   ........T.R.U.E.
5FCC40   00 00 00 00 4A 00 93 00  07 00 04 00 30 00 08 02   ....J.▮.....0...
5FCC50   B0 EC 04 02 80 93 DD 01  01 00 00 00 F9 BA 0C 02   °ì..▮▮Ý.....ùº..
5FCC60   20 38 1C 01 00 00 00 00  B0 D7 DC 01 00 00 00 00    8......°×Ü.....
5FCC70   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
5FCC80   03 00 07 00 29 01 08 02  B0 4B 9E 00 80 4B 9E 00   ....)...°K▮.▮K▮.
5FCC90   01 00 00 00 C0 5C A9 00  0C 00 03 00 2A 01 0C 02   ....À\©.....*...
5FCCA0   F8 9C 18 02 6E 61 6D 65  3D 6A 73 6D 69 74 68 26   ø▮..name=jsmith&
5FCCB0   70 61 73 73 77 6F 72 64  3D 70 61 73 73 31 32 33   password=pass123
5FCCC0   34 26 4C 6F 67 69 6E 5F  78 3D 4C 6F 67 69 6E 26   4&Login_x=Login&
5FCCD0   75 69 64 3D 34 34 65 34  64 39 65 31 30 32 66 31   uid=44e4d9e102f1
5FCCE0   38 31 31 35 35 38 34 38  36 37 33 26 6D 64 70 61   81155848673&mdpa
5FCCF0   73 73 3D 00 69 6C 2F 00  11 00 0C 00 26 01 08 02   ss=.il/.....&...
5FCD00   38 50 07 02 90 94 EC 01  00 00 00 00 00 00 00 00   8P..▮▮ì.........
5FCD10   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
5FCD20   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
5FCD30   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
5FCD40   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
5FCD50   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
5FCD60   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
5FCD70   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
5FCD80   04 00 11 00 09 01 08 02  00 DF B4 01 30 17 94 59   .........ß´.0.▮Y
```

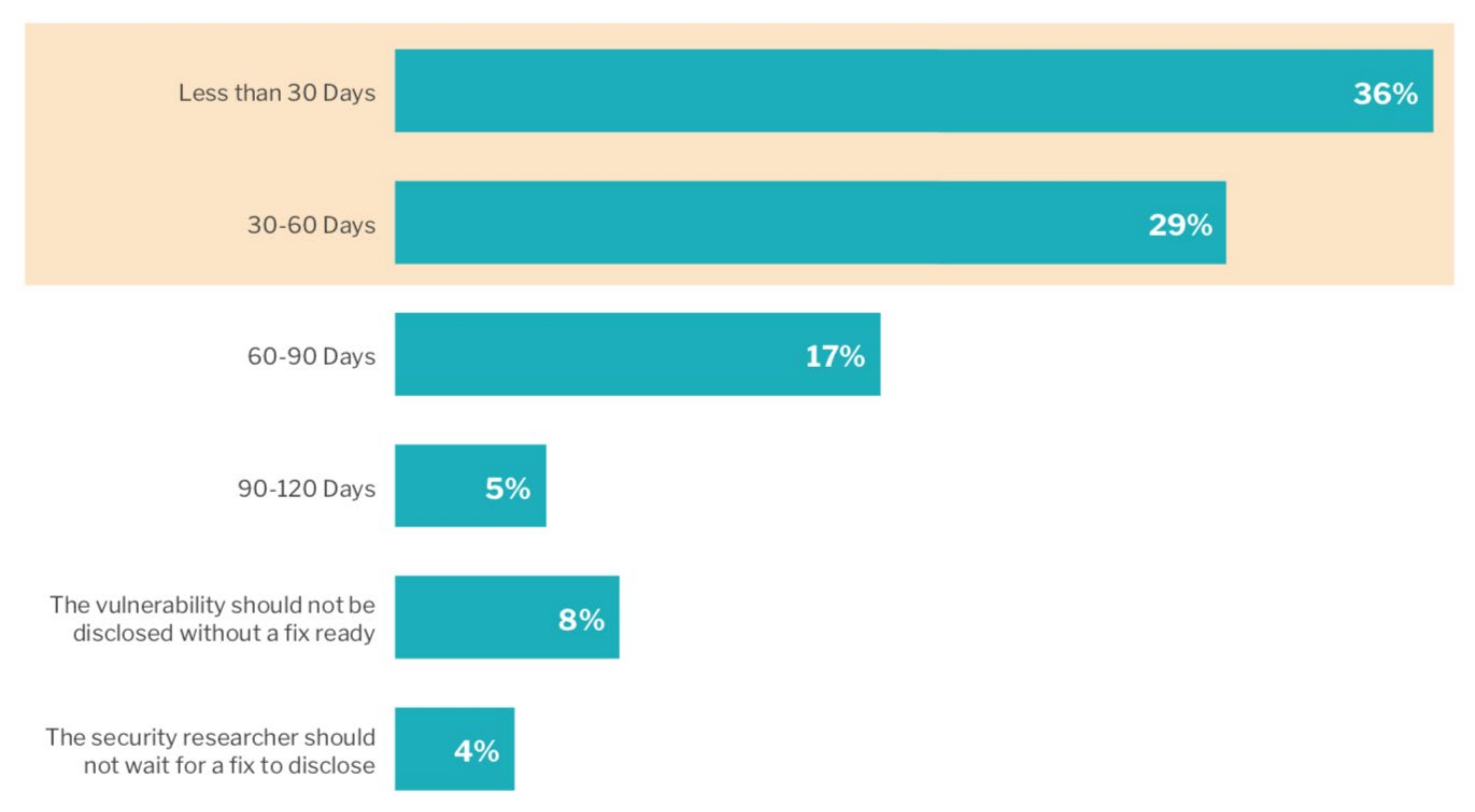
Page 23717 of 81955 = 112 Block: n/a Size: n/a

User ID/password cached in memory indefinitely

Actions that researchers take now



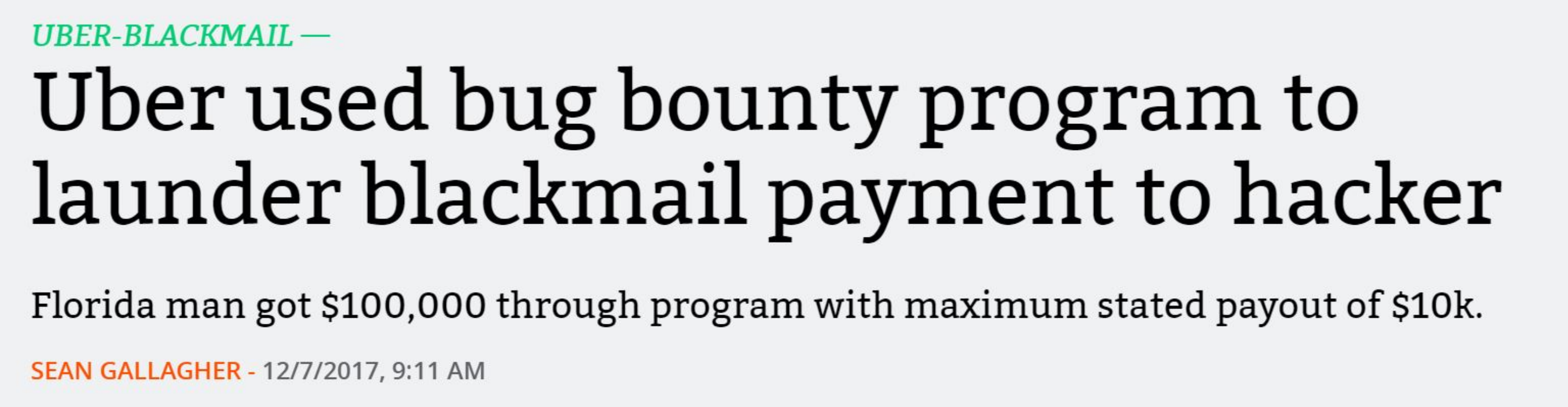
What's an appropriate time frame for a vendor to correct a vulnerability once notified, before the security researcher discloses it?



Sentiment has changed over the years

- Most (**90%**) respondents see vulnerability disclosure as a public good, that the identification of vulnerabilities increases transparency and is good for the overall security posture for everyone.
- A majority, **62%**, do not think prior permission from a product or application owner is required.

Safe Harbor:
I Do Not Think It Means What You Think It Means

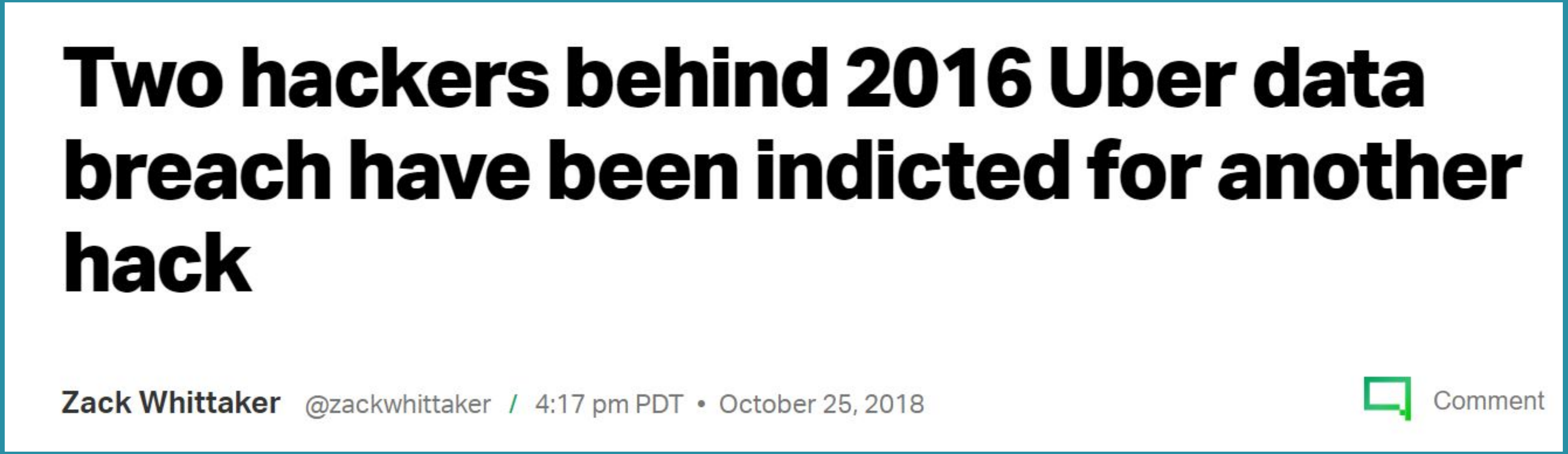


UBER-BLACKMAIL —

Uber used bug bounty program to launder blackmail payment to hacker

Florida man got $100,000 through program with maximum stated payout of $10k.

SEAN GALLAGHER - 12/7/2017, 9:11 AM



Two hackers behind 2016 Uber data breach have been indicted for another hack

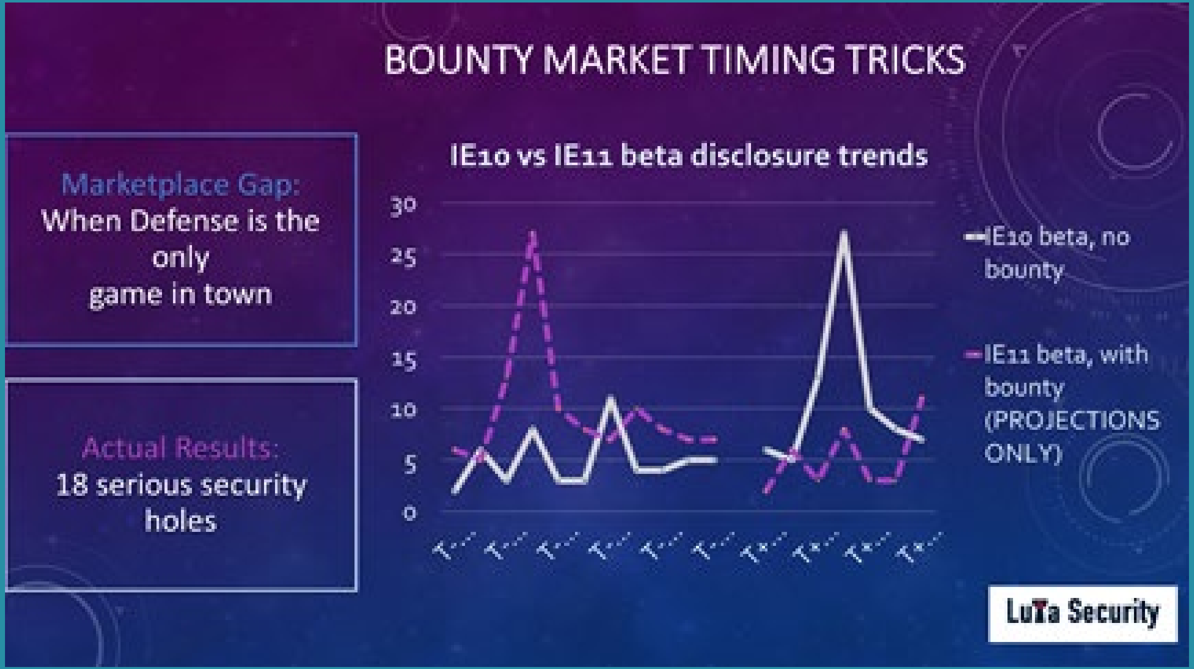
Zack Whittaker @zackwhittaker / 4:17 pm PDT • October 25, 2018

CVD Goes Mainstream!

Companies with
Bug Bounty Programs
Google
Mozilla
(Firefox)
Facebook
Microsoft
PayPal
Etsy

Companies with
Bug Bounty Programs
Google
Mozilla
(Firefox)
Facebook
Microsoft
PayPal
Etsy

MS Bug Bounties 2013: Bounty Smarter, Not Harder

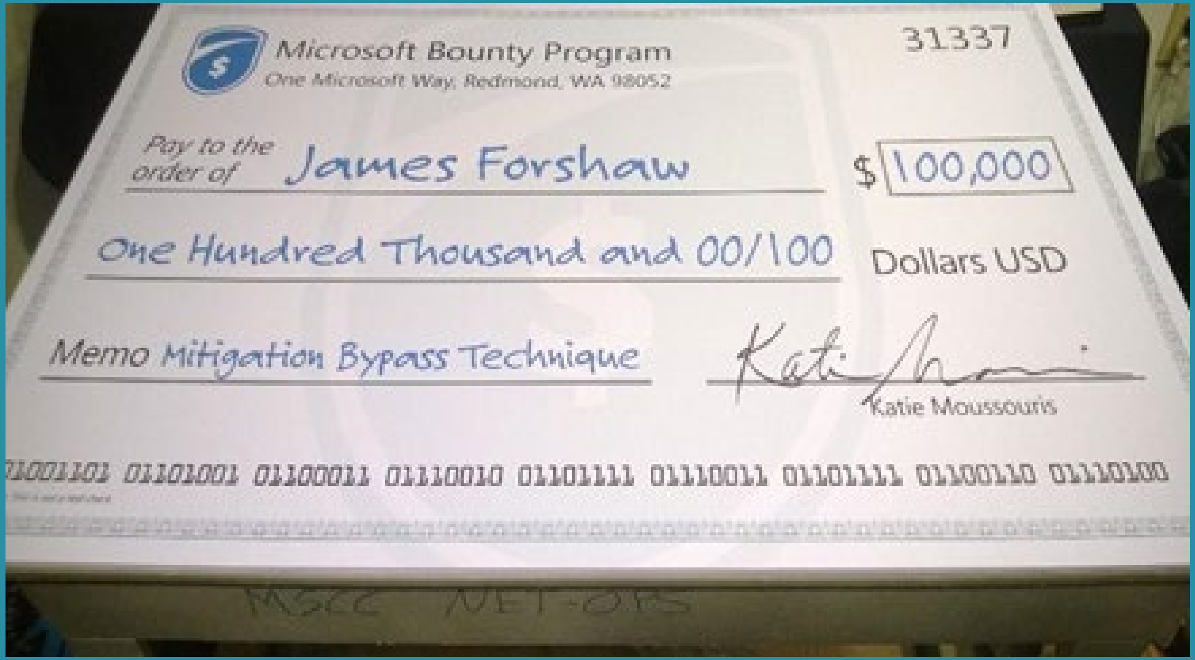


BOUNTY MARKET TIMING TRICKS

Marketplace Gap:
When Defense is the only
game in town

Actual Results:
18 serious security holes

IE10 vs IE11 beta disclosure trends



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

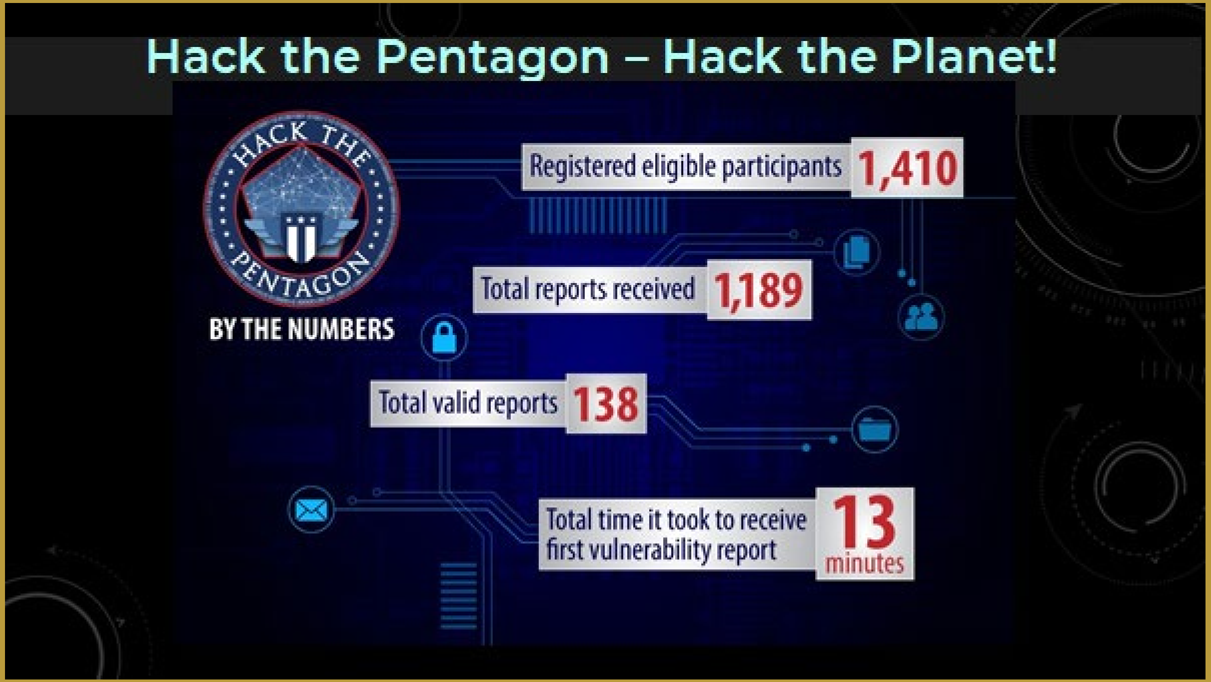
Kati

Katie Moussouris

1001101 01101001 01100011 01110010 01101111 01110011 01101111 01100110 01110100

A couple of Facebook bug bounty stories

Hack the Pentagon - Hack the Planet!

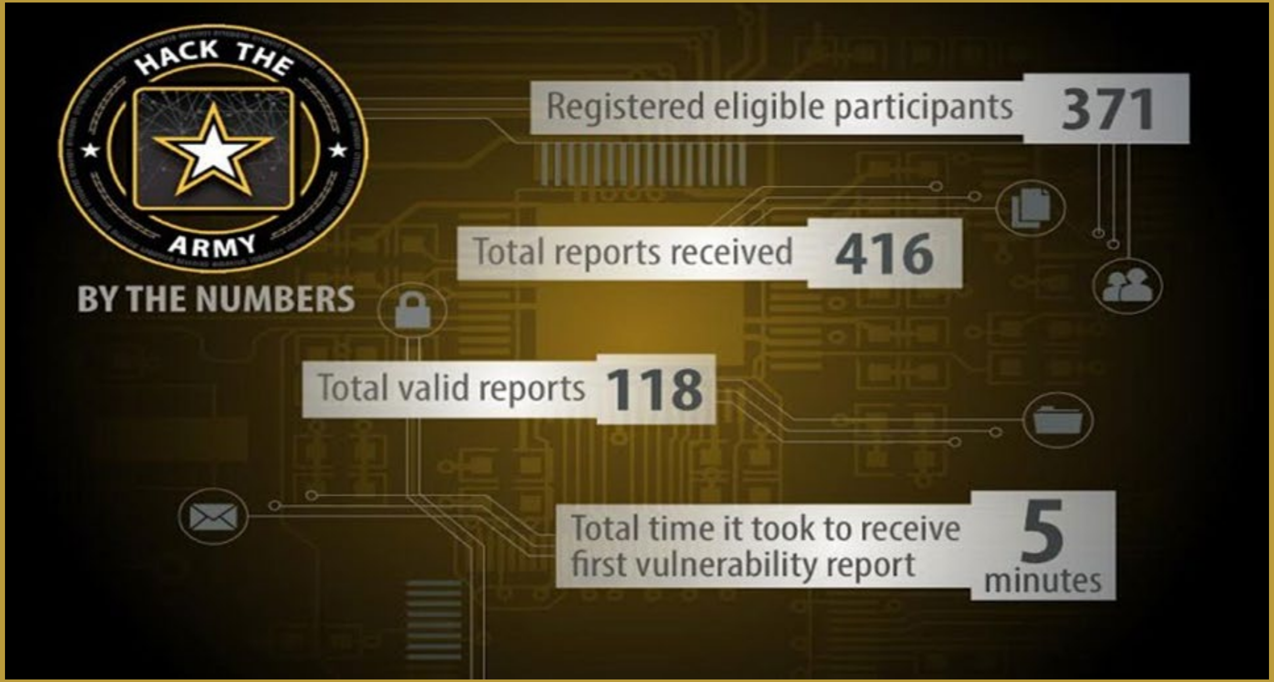


Hack the Pentagon – Hack the Planet!

HACK THE PENTAGON

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

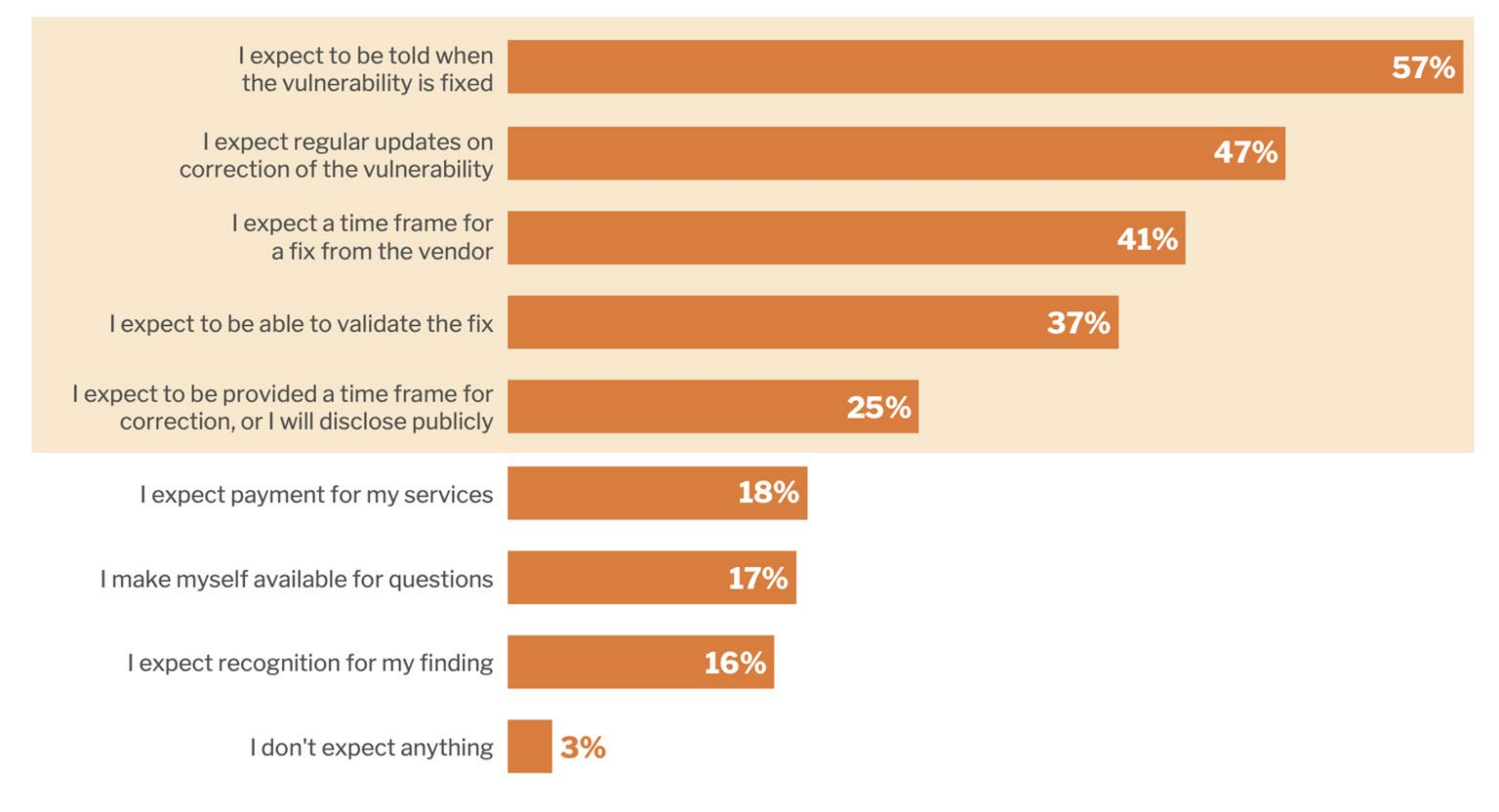
BY THE NUMBERS

Registered eligible participants	371
Total reports received	416
Total valid reports	118
Total time it took to receive first vulnerability report	5 minutes

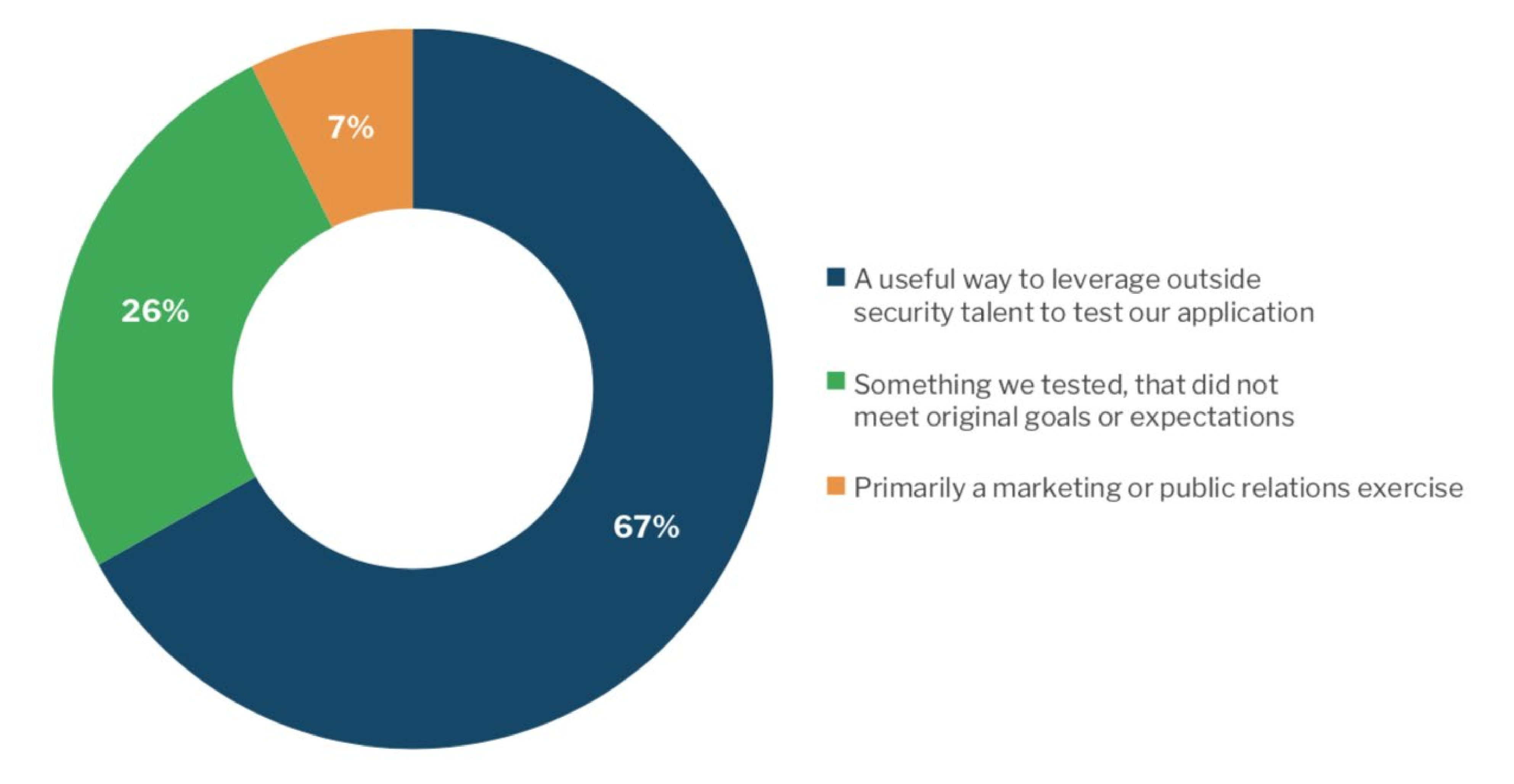
April 2016: Come At Me!

November 2016: Hack Me Gently With A Chainsaw

What do researchers expect?

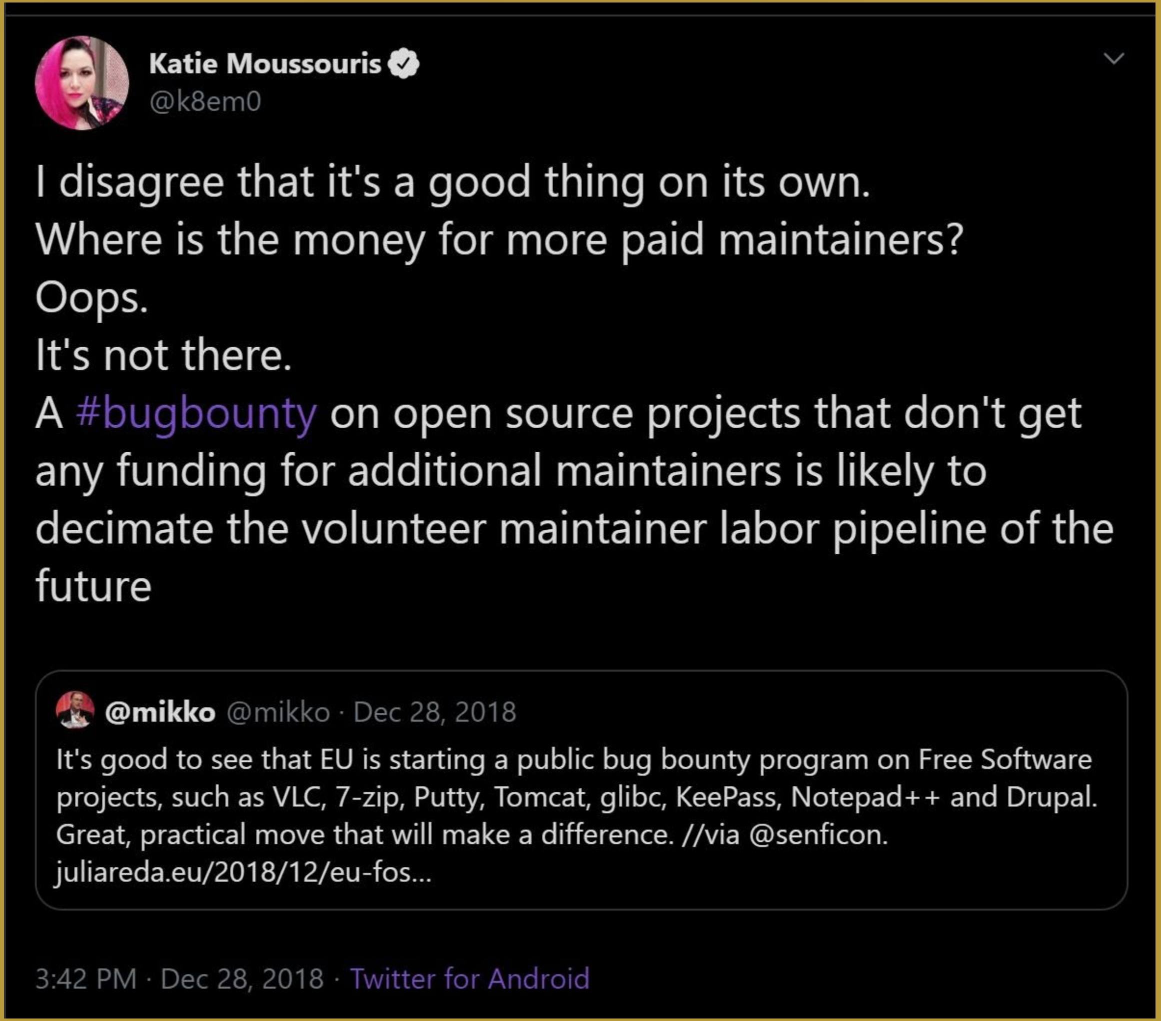


47% of participants had worked with bug bounties. This is what they thought.



Knowing About Bugs is 1/100th of the Battle

- Nearly half (47%) of organizations have implemented bug bounty programs, but they say that only 19% of vulnerability reports come via bug bounty programs.
- Only 63% of open source vulnerabilities reported are being fixed.



Katie Moussouris
@k8em0

I disagree that it's a good thing on its own.
Where is the money for more paid maintainers?
Oops.
It's not there.
A #bugbounty on open source projects that don't get any funding for additional maintainers is likely to decimate the volunteer maintainer labor pipeline of the future

@mikko @mikko · Dec 28, 2018
It's good to see that EU is starting a public bug bounty program on Free Software projects, such as VLC, 7-zip, Putty, Tomcat, glibc, KeePass, Notepad++ and Drupal. Great, practical move that will make a difference. //via @senficon. juliareda.eu/2018/12/eu-fos...

3:42 PM · Dec 28, 2018 · Twitter for Android

So you say you’ve come a long way.

The process is mostly working!

- **Three out of four** organizations report having an established method for receiving vulnerability reports from security researchers.
- For those organizations that received an unsolicited vulnerability report, **90%** of vulnerabilities were disclosed in a coordinated fashion between security researchers and organizations.
- More than one-third (37%) of organizations have received an unsolicited disclosure report in the past 12 months.

Apply What You Have Learned Today

- Next week you should:
  - **Assess your internal process maturity** in handling existing or publicly disclosed bugs. **Can you handle the truth**?!
  - Understand if your organization has a **CVD policy** with a contact. If not, get one created.
- In the first three months following this presentation you should:
  - Create a **response process** to handle incoming researcher disclosures.
- Within six months you should:
  - If you build any applications and aren't performing security testing in your **SDLC** start!
  - Start the journey to a **full SDLC security process from threat modeling** to rapid response.

Resources & Links

ISO 29147: https://www.iso.org/standard/72311.html

ISO 30111: https://www.iso.org/standard/69725.html

Veracode & 451 Research CVD Study 2019: https://info.veracode.com/survey-report-451-research-exploring-coordinated-disclosure.html

20-minute ISO Standards Overview Video: https://www.youtube.com/watch?v=-L3DNZtK8lc

Uber Senate Hearing: https://www.commerce.senate.gov/public/?a=Files.Serve&File_id=E162FD54-F858-44AE-B25F-64E331C628AE

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

CVD Maturity Model: https://www.rsaconference.com/writable/presentations/file_upload/ht-r04f-but_now_i_see_-_a_vulnerability_disclosure_maturity_model.pdf

Vuln/Exploit Market Dynamics::

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	CWysopal at Veracode dot com
@LutaSecurity @k8em0	@veracode @weldpond

RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **KEY-F01S**

Coordinated Vulnerability Disclosure: You’ve Come a Long Way, Baby

Katie Moussouris

Founder & CEO
Luta Security
@k8em0

Chris Wysopal

Co-founder @ CTO
Veracode
@WeldPond

#RSAC