CROWDSOURCED SECURITY KEEPS US RESILIENT

YES WE H/CK

GLOBAL BUG BOUNTY & VDP PLATFORM

EILEEN NEO

APAC REGIONAL LEAD

YES WE HACK

PAY A REWARD NOT A RANSOM

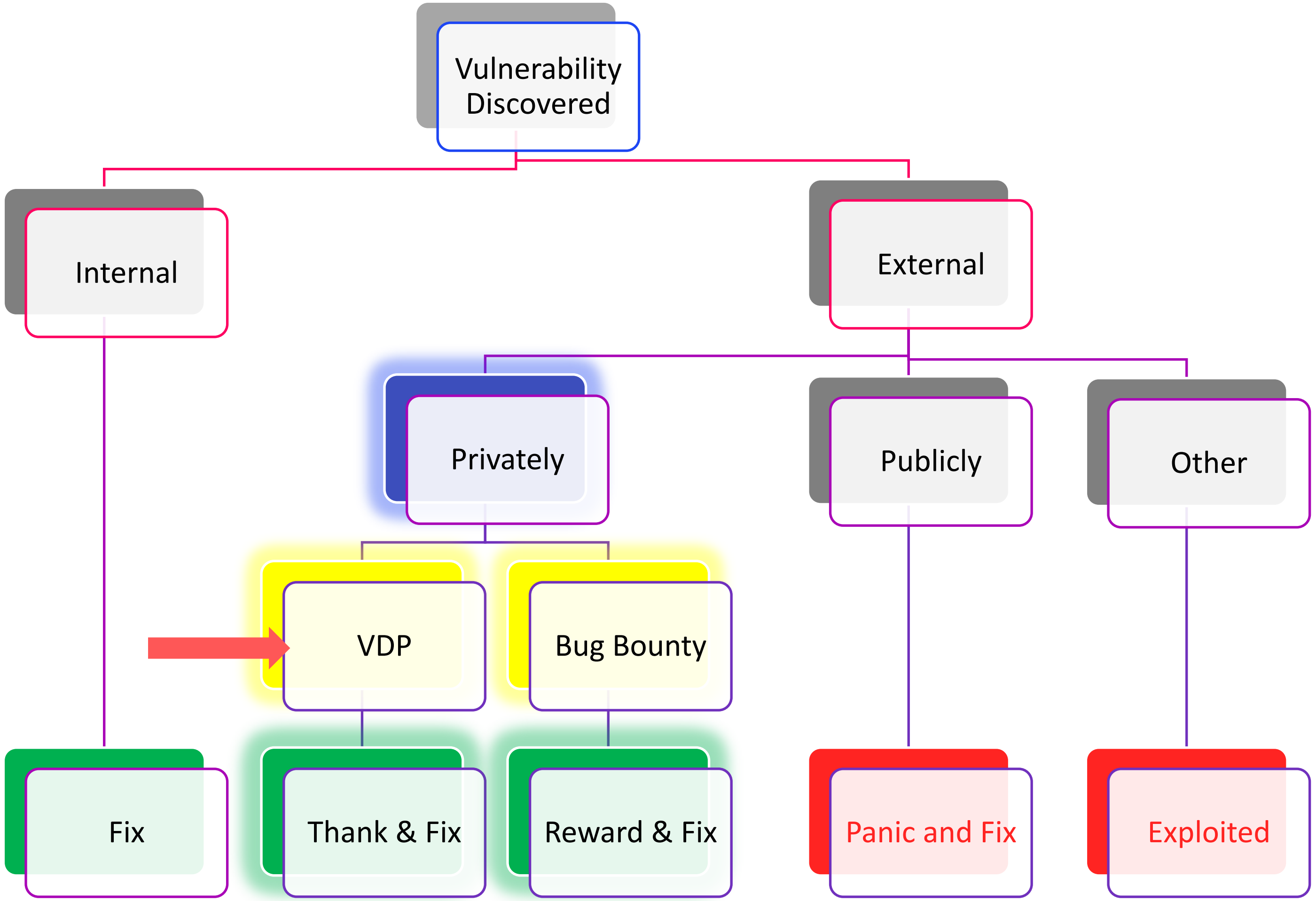
YES WE HACK

- Global Bug Bounty & VDP Platform
- 400+ programs – public & private
- 30+ countries
- 30,000+ vetted researchers

CROWDSOURCED SECURITY

VULNERABILITY DISCLOSURE POLICY + BUG BOUNTY

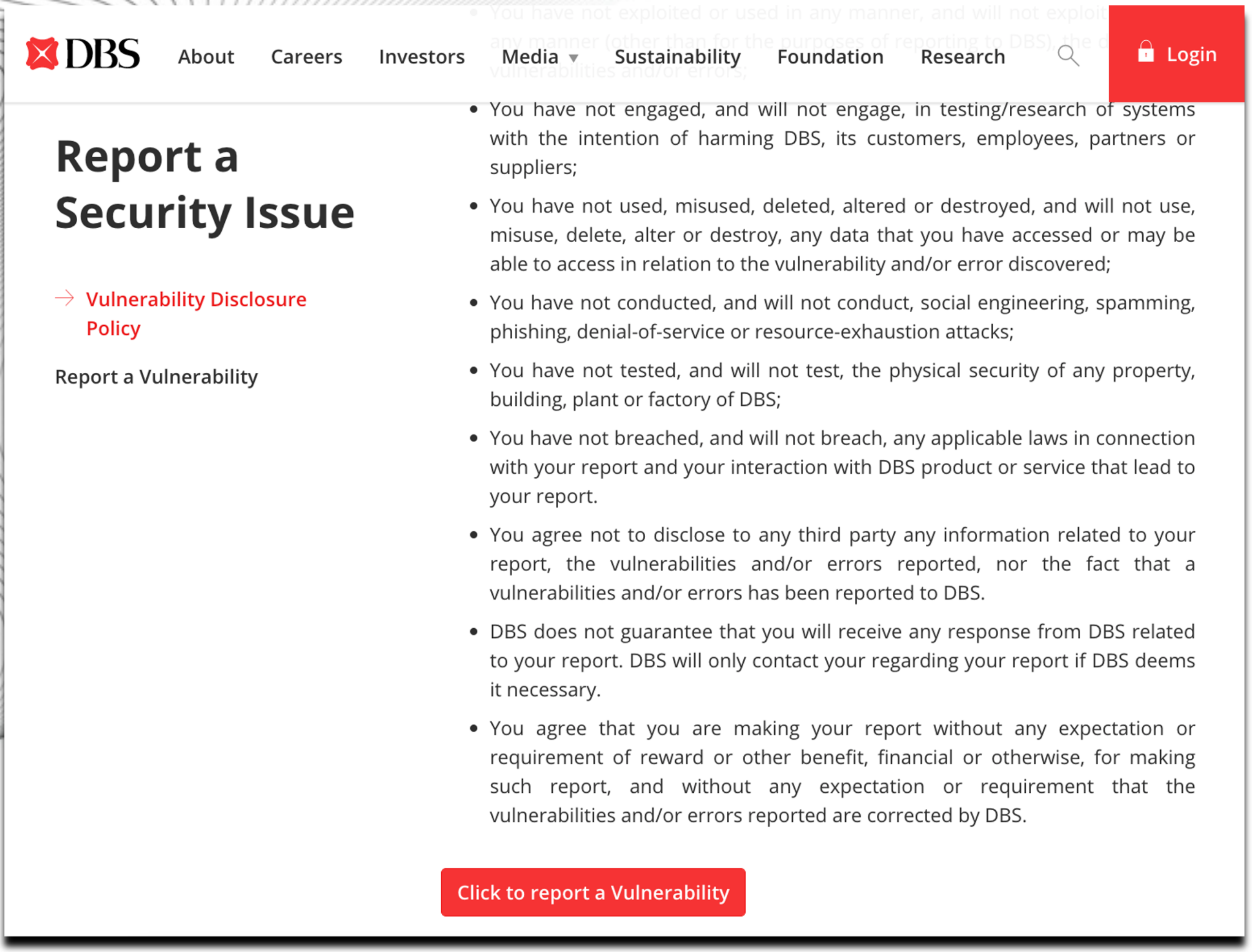
- Vulnerabilities are exploitable by hackers to cause damage.
- With the increase in digitalization and attack surface, the increase in attackers, how can we keep up with just a few employees and pentesters?



YES WE H/CK

WHAT IS VDP?

VULNERABILITY DISCLOSURE POLICY



- You have not exploited or used in any manner, and will not exploit ... any manner (other than for the purposes of reporting to DBS), the ... vulnerabilities and/or errors;

Report a Security Issue

→ Vulnerability Disclosure Policy

Report a Vulnerability

- You have not engaged, and will not engage, in testing/research of systems with the intention of harming DBS, its customers, employees, partners or suppliers;
- You have not used, misused, deleted, altered or destroyed, and will not use, misuse, delete, alter or destroy, any data that you have accessed or may be able to access in relation to the vulnerability and/or error discovered;
- You have not conducted, and will not conduct, social engineering, spamming, phishing, denial-of-service or resource-exhaustion attacks;
- You have not tested, and will not test, the physical security of any property, building, plant or factory of DBS;
- You have not breached, and will not breach, any applicable laws in connection with your report and your interaction with DBS product or service that lead to your report.
- You agree not to disclose to any third party any information related to your report, the vulnerabilities and/or errors reported, nor the fact that a vulnerabilities and/or errors has been reported to DBS.
- DBS does not guarantee that you will receive any response from DBS related to your report. DBS will only contact your regarding your report if DBS deems it necessary.
- You agree that you are making your report without any expectation or requirement of reward or other benefit, financial or otherwise, for making such report, and without any expectation or requirement that the vulnerabilities and/or errors reported are corrected by DBS.

Click to report a Vulnerability

/ A public channel for anyone to report a bug directly to the security team.

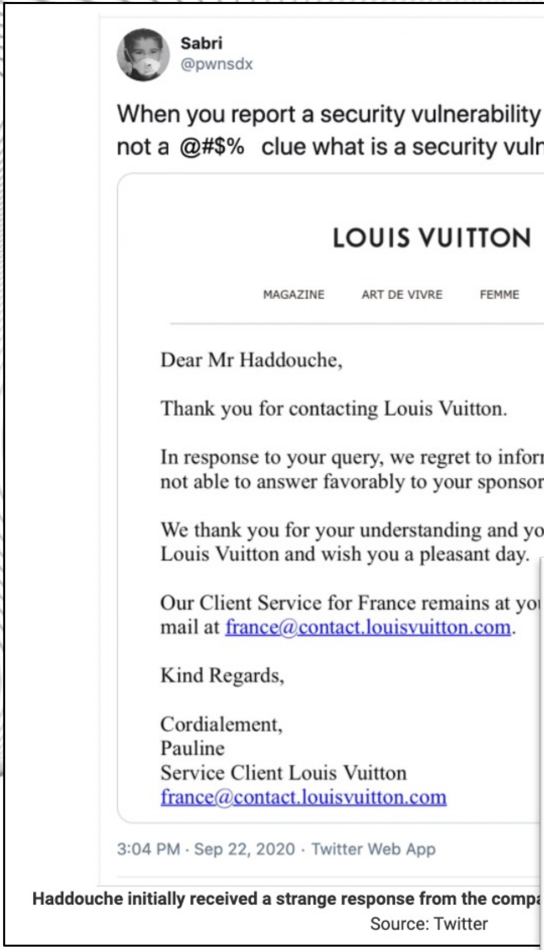
/ There are many goodwill security researchers who have found bugs and need a safe and clear framework to inform you. (Fear of unfair prosecution)

/ Without a process to receive bugs securely, organisations will miss out on important information.

YES WE H/CK

WHAT IS VDP?

VULNERABILITY DISCLOSURE POLICY



Sabri
@pwnsdx

When you report a security vulnerability but they have not a @#$% clue what is a security vulnerability

LOUIS VUITTON

MAGAZINE ART DE VIVRE FEMME HOMME

Dear Mr Haddouche,

Thank you for contacting Louis Vuitton.

In response to your query, we regret to inform you that we are not able to answer favorably to your sponsorship proposal.

We thank you for your understanding and your interest in Louis Vuitton and wish you a pleasant day.

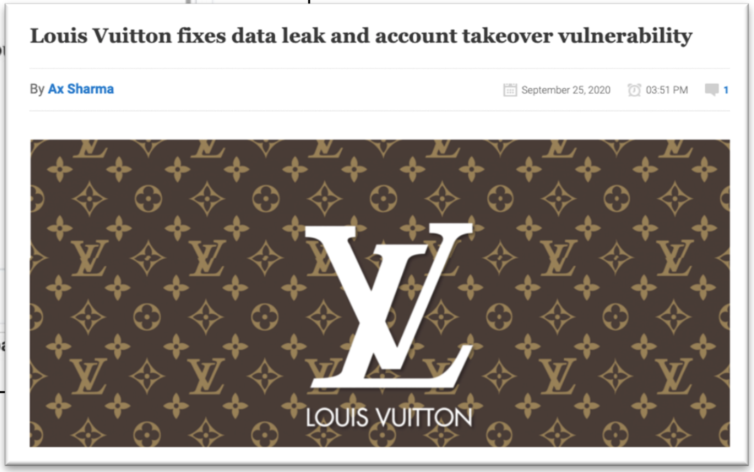
Our Client Service for France remains at yo
mail at france@contact.louisvuitton.com.

Kind Regards,

Cordialement,
Pauline
Service Client Louis Vuitton
france@contact.louisvuitton.com

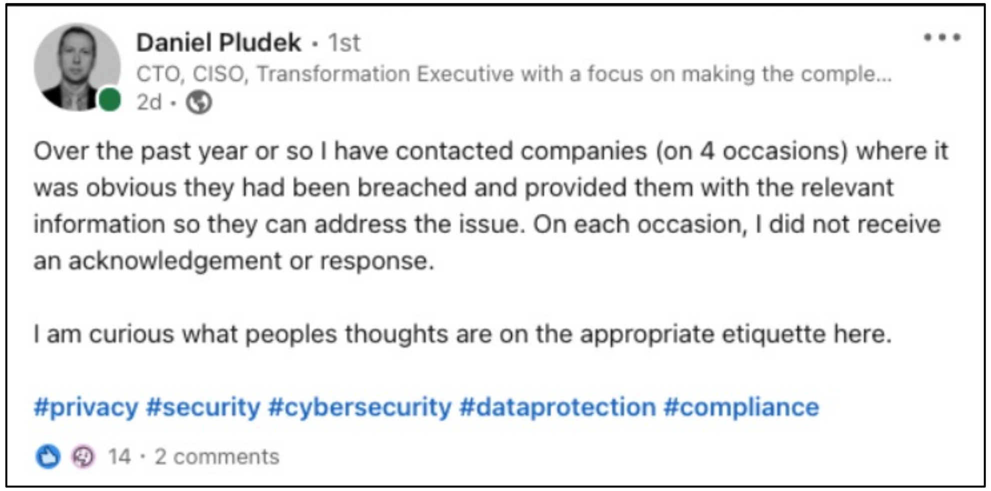
3:04 PM · Sep 22, 2020 · Twitter Web App

Haddouche initially received a strange response from the compa
Source: Twitter



Louis Vuitton fixes data leak and account takeover vulnerability

By Ax Sharma September 25, 2020 03:51 PM 1



Daniel Pludek • 1st
CTO, CISO, Transformation Executive with a focus on making the comple...
2d •

Over the past year or so I have contacted companies (on 4 occasions) where it was obvious they had been breached and provided them with the relevant information so they can address the issue. On each occasion, I did not receive an acknowledgement or response.

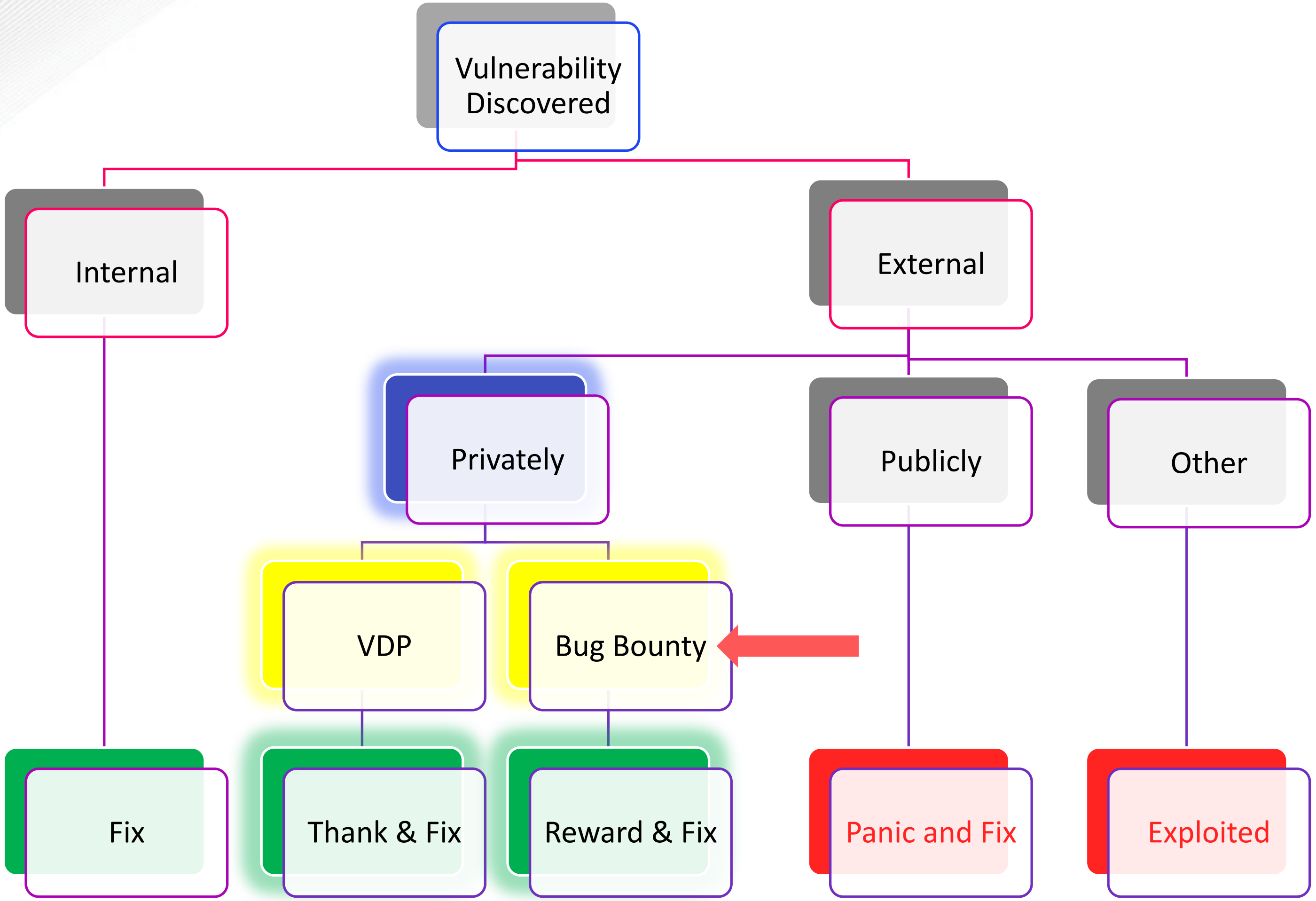
I am curious what peoples thoughts are on the appropriate etiquette here.

#privacy #security #cybersecurity #dataprotection #compliance

14 · 2 comments

CROWDSOURCED SECURITY

VULNERABILITY DISCLOSURE POLICY + BUG BOUNTY

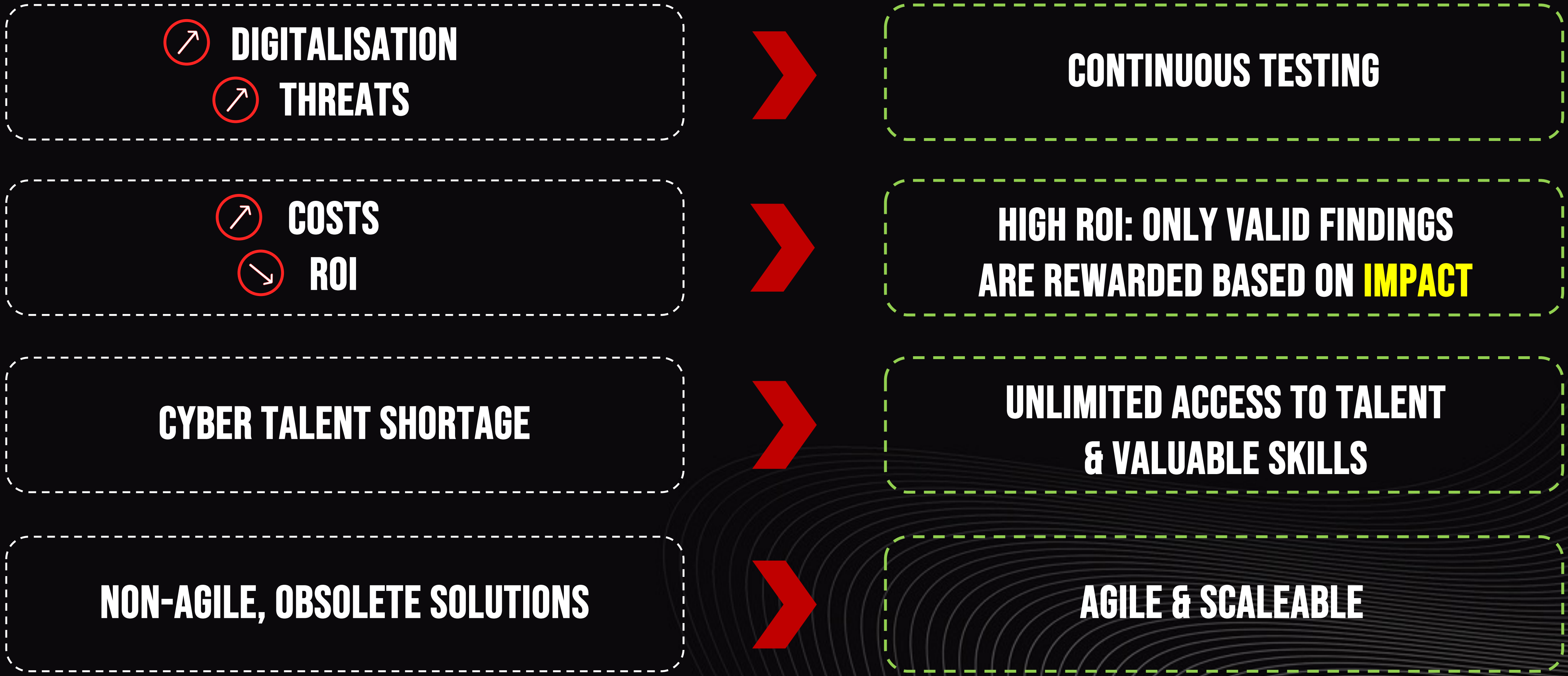


YES WE H/CK

NOT DOING ENOUGH TO DISCOVER VULNERABILITIES

PROBLEM	Widening attack surface	Malicious actors trying to hack into companies 24/7	Overwhelmed with bugs and not able to keep up
UNFORTUNATELY	Testing once a year / infrequently	Limited pentesters	Paid on manhours, not results
WE NEED TO	Test more frequently	Get diverse perspectives into our security	Incentivise testers to find bugs

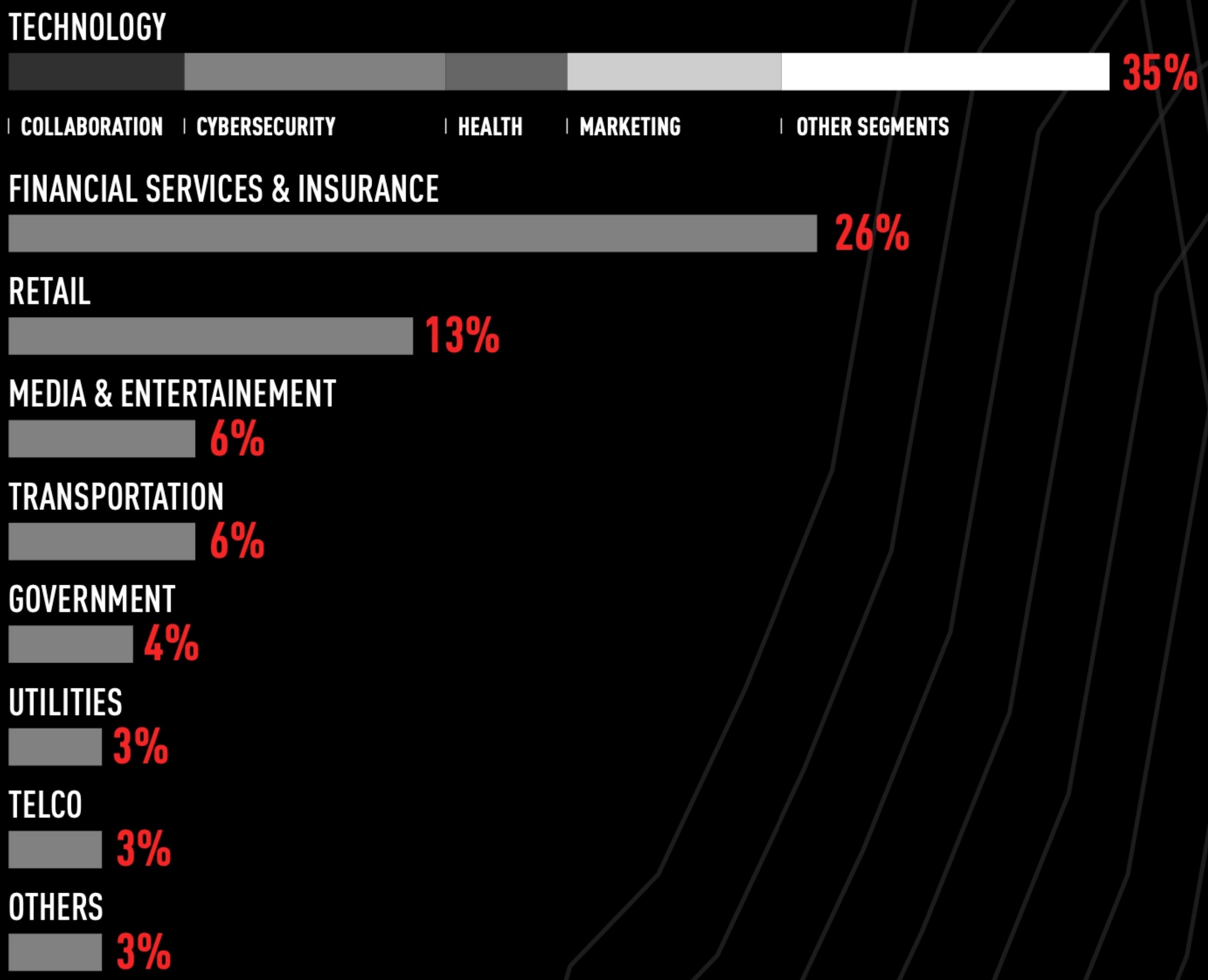
FIGHT DYNAMIC THREATS WITH THE RIGHT TOOLS



↗ DIGITALISATION ↗ THREATS	CONTINUOUS TESTING
↗ COSTS ↘ ROI	HIGH ROI: ONLY VALID FINDINGS ARE REWARDED BASED ON **IMPACT**
CYBER TALENT SHORTAGE	UNLIMITED ACCESS TO TALENT & VALUABLE SKILLS
NON-AGILE, OBSOLETE SOLUTIONS	AGILE & SCALEABLE

Crowdsourced security for all

Bug Bounty is gaining fast traction across industries



Trust

2020, a year of exponential growth

120%

INCREASE IN PROGRAMS YEAR-OVER-YEAR

x2

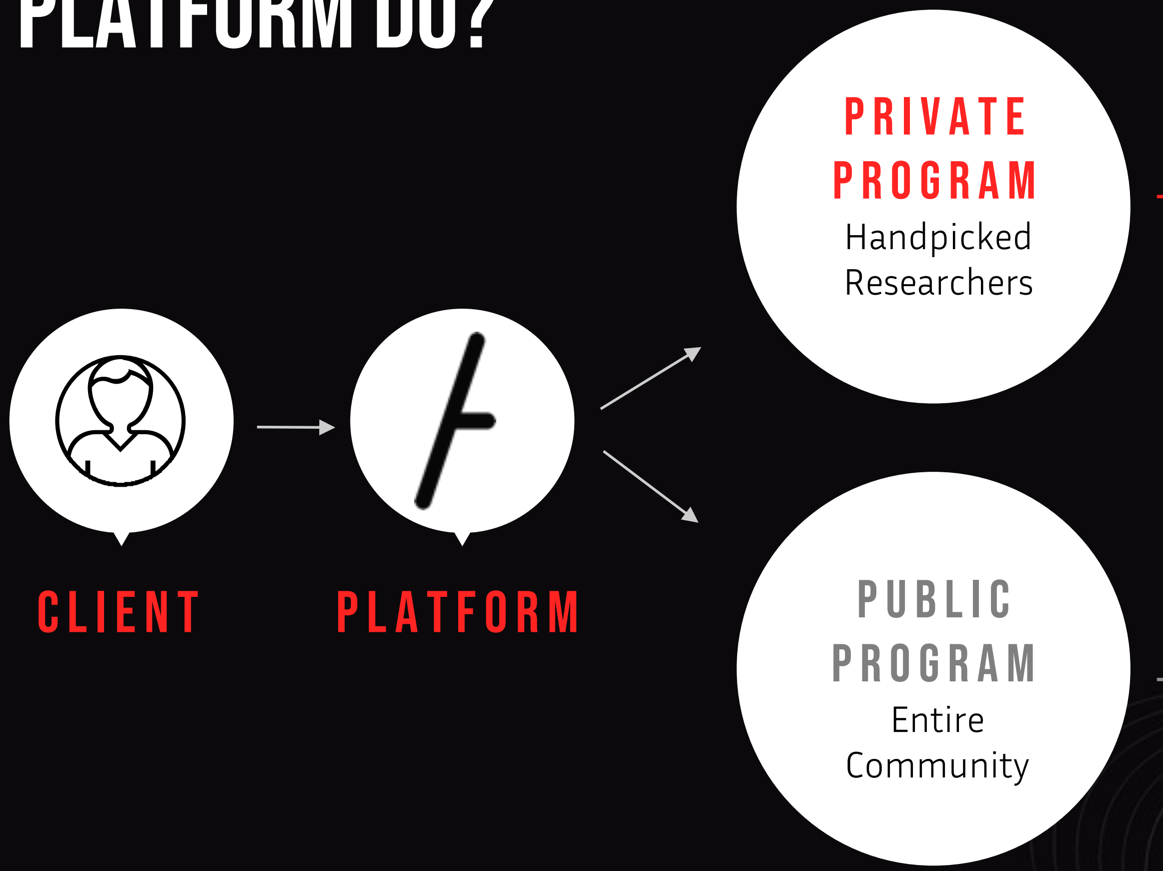
THE AMOUNT OF IDENTIFIED VULNERABILITIES MORE THAN DOUBLED

WHAT IS BUG BOUNTY?

CROWDSOURCING APPLIED TO CYBERSECURITY

- Reward researchers with bounties for the vulnerabilities (bugs) they report.
- Follows strict rules to find bugs within defined scopes.
- Rewarded based on bug severity, and a defined rewards grid.

WHAT DOES A BUG BOUNTY PLATFORM DO?



CLIENT

PLATFORM

PRIVATE PROGRAM

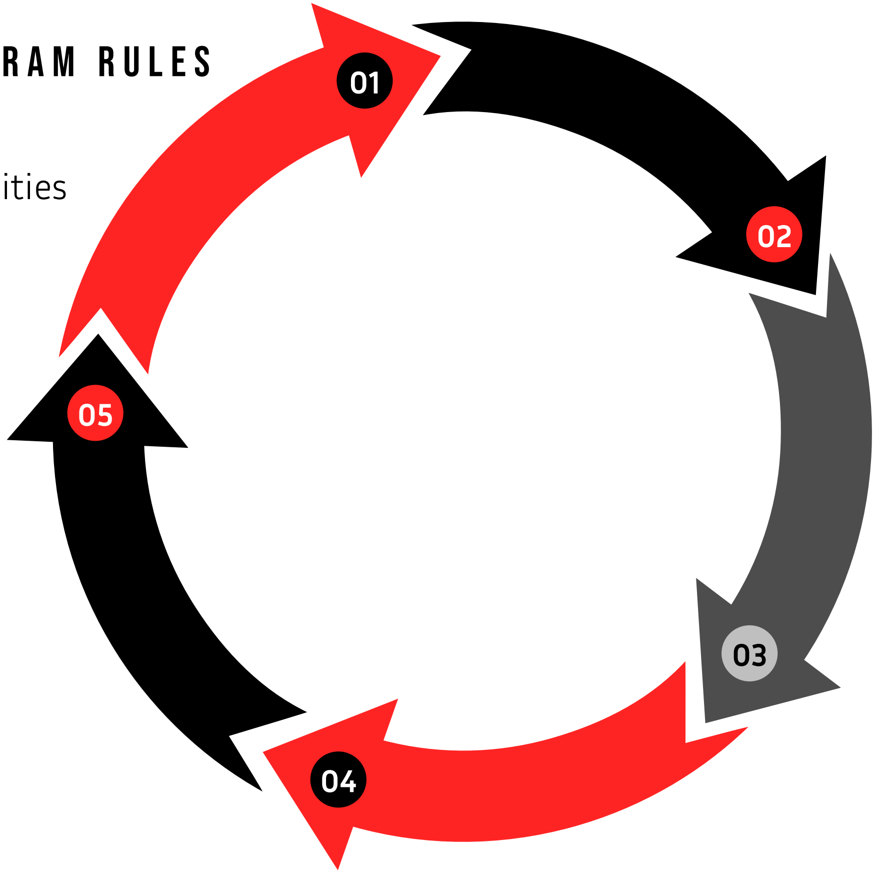
Handpicked Researchers

PUBLIC PROGRAM

Entire Community

YES WE H/CK

HOW A BUG BOUNTY PROGRAM WORKS



SET UP YOUR PROGRAM RULES

- Scope
- Qualifying vulnerabilities
- Rewards grid

LAUNCH YOUR PROGRAM

- Private: to a selection of hunters
- Public: to the whole community

TRIAGE REPORTS

- Qualification vs. Rules
- Severity Level
- Validation

PAY REWARDS

FIX & CHECK

VDP VS BUG BOUNTY

VDP = PASSIVE APPROACH

- WHY: Receive bugs from the public
- HOW: Set up a communication channel on your website / a dedicated webpage
- WHO: For anyone wishing to report a bug

A 'THANKS' FOR CIVIC DUTY

- No expectation of financial reward
- Discovery by chance

COMMITMENT TO SECURITY

BUG BOUNTY = ACTIVE APPROACH

- WHY: Encourage active vulnerability research
- HOW: Set up a detailed programme (*scopes, rules & reward grid)*
- WHO: YesWeHack Professional Community

REWARDS

- Attracted by a financial reward
- Active research

IMPROVE YOUR SECURITY

CONCLUSION

Old security testing models are **no longer effective** in this ”new-normal”.

How can we continue to defend an ever-increasing attack surface, a more active cybercrime world, with tight budgets and a small security team?

Bug Bounty and Crowdsourced Security can no longer be ignored. The question is no longer whether to run a Bug Bounty program or not, but **when or where to start**.

YES WE HACK

THANK YOU

EILEEN NEO

E.NEO@YESWEHACK.COM