Duration: 20 min | Virtual Event | Cyber Workforce Summit | Oct. 28th , 2021

Setting Sail on Security Research

Dave Alen | zumaroc.com

zumaroc

Discussion overview

In this activity we are going to explore why some believe "…ethical hacking [or security researching] is the coolest job in tech right now." [1]

Learning objectives

- Understand the inspiration behind security research
- Actions of the security researcher
- The impact of security research [MTN Group as case study]
- How do you get started?

Keywords

Security Researcher*, Bug Bounty, Bugs, Crowdsourced Security Platform, Bug Bounty Platform, Vulnerability Disclosure* Program (*VDP*), Cyber-resilient organization

1. The inspiration behind security research

3 min

The Digital World

- *Nothing is **immune**.*

- ***security research** is the closest we have to immunity, so it makes sense that individuals get **rewarded.***

- *The "**democratization**" of bug bounty programs, will reduce ransomware.*

The Real World

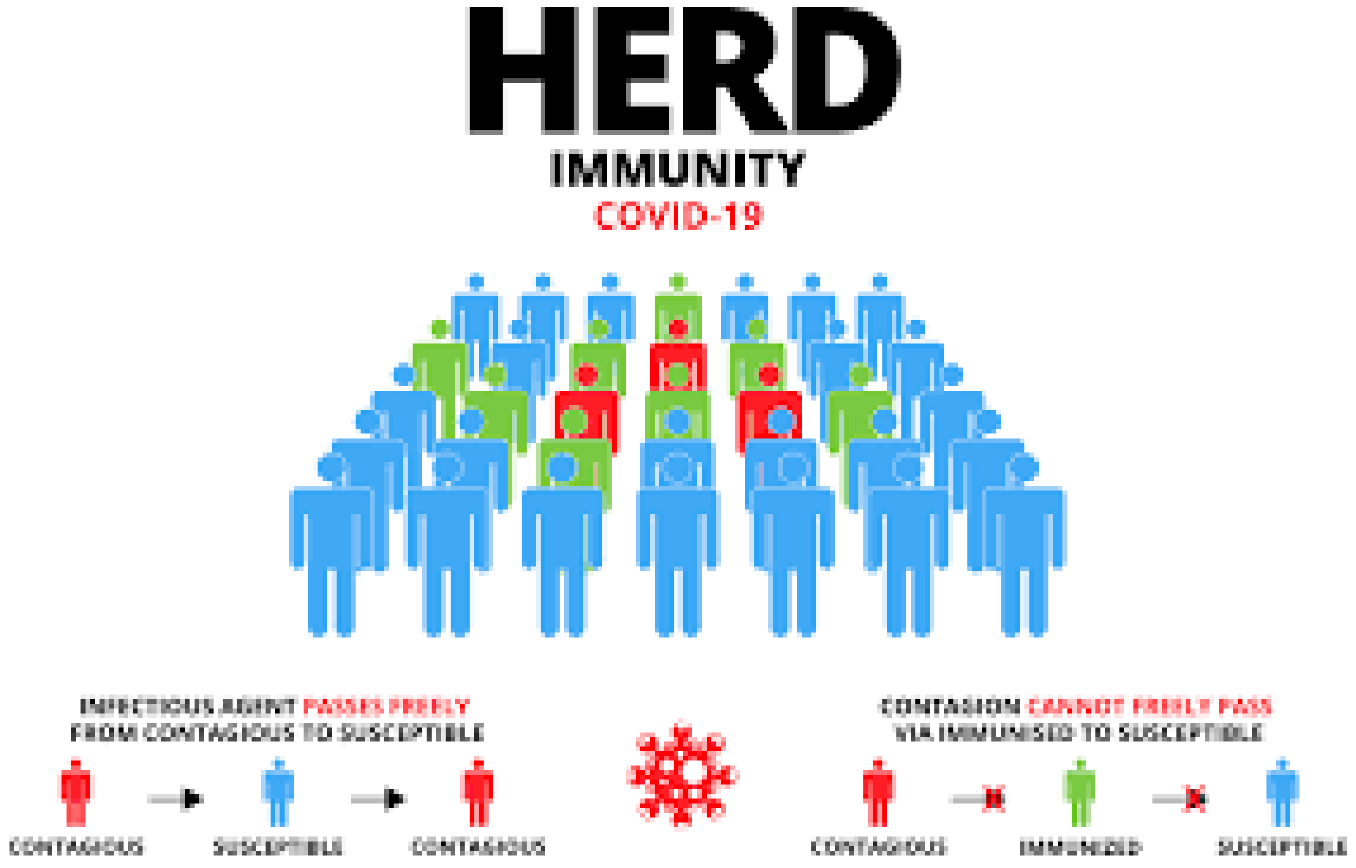

HERD
IMMUNITY
COVID-19
INFECTIOUS AGENT PASSES FREELY FROM CONTAGIOUS TO SUSCEPTIBLE
CONTAGIOUS
SUSCEPTIBLE
CONTAGIOUS
CONTAGION CANNOT FREELY PASS VIA IMMUNISED TO SUSCEPTIBLE
CONTAGIOUS
IMMUNIZED
SUSCEPTIBLE

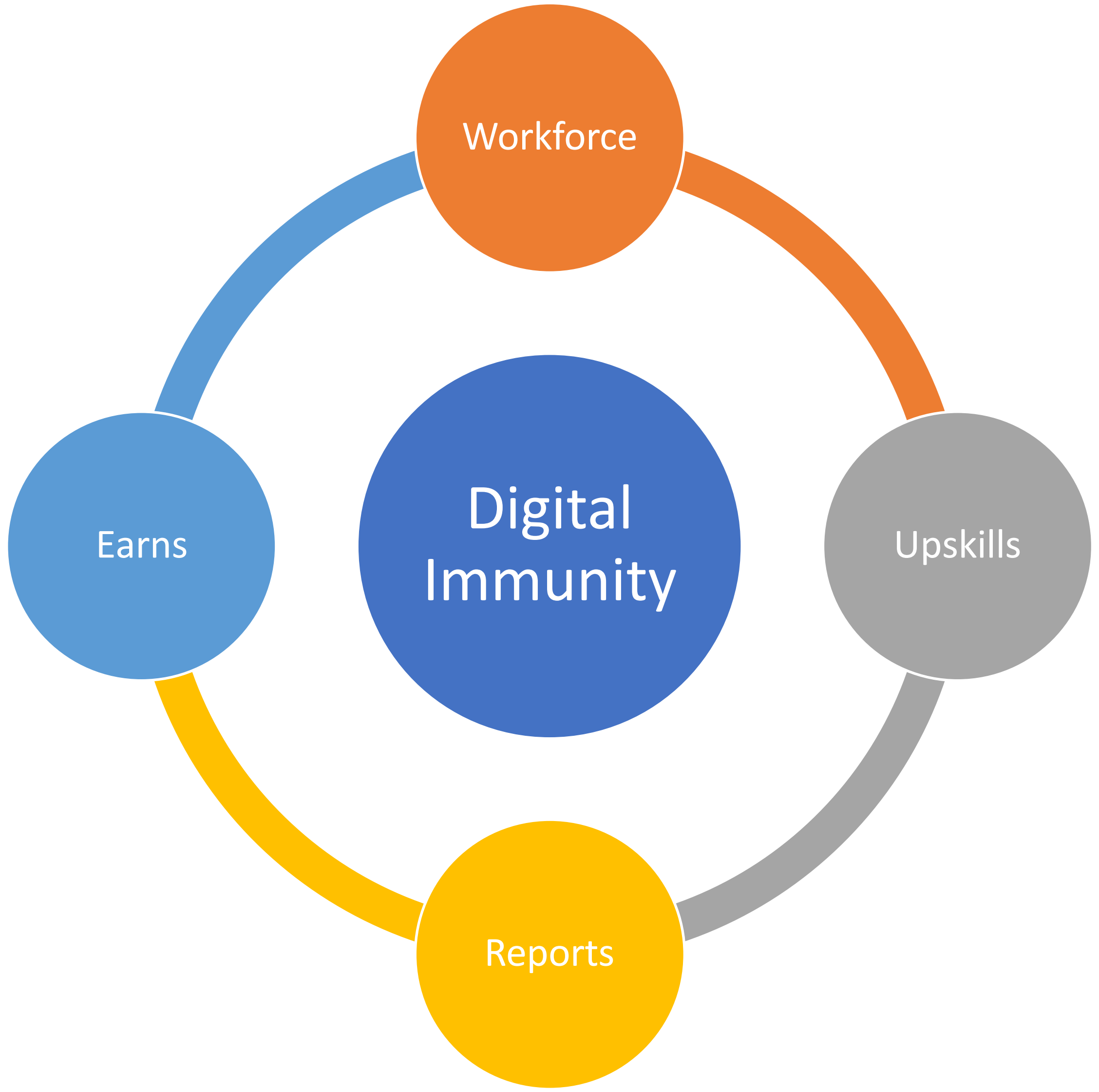
Image Source: https://www.narayanahealth.org/

Zumaroc

2. Actions of the security researcher

3 min

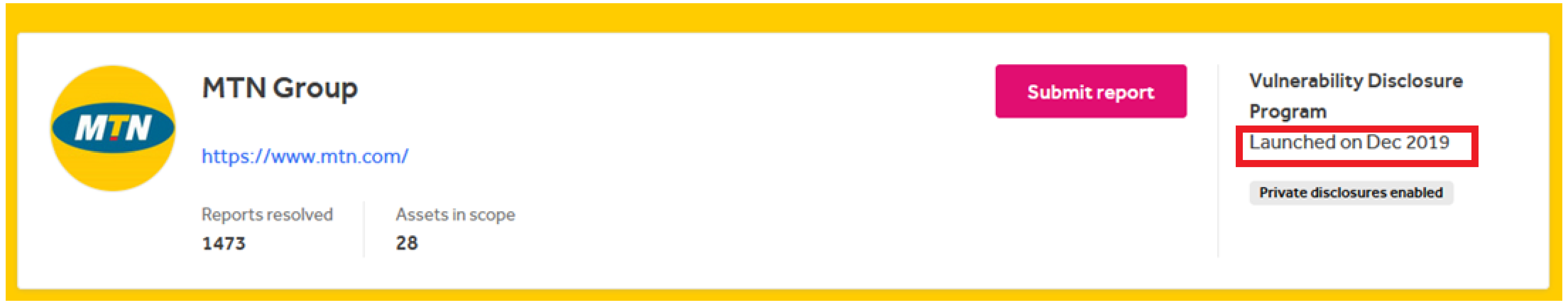
They report bugs to earn rewards and make the digital world a better place



Zumaroc

3a. The impact of security research – MTN

3 min



MTN Group

https://www.mtn.com/

Reports resolved
1473

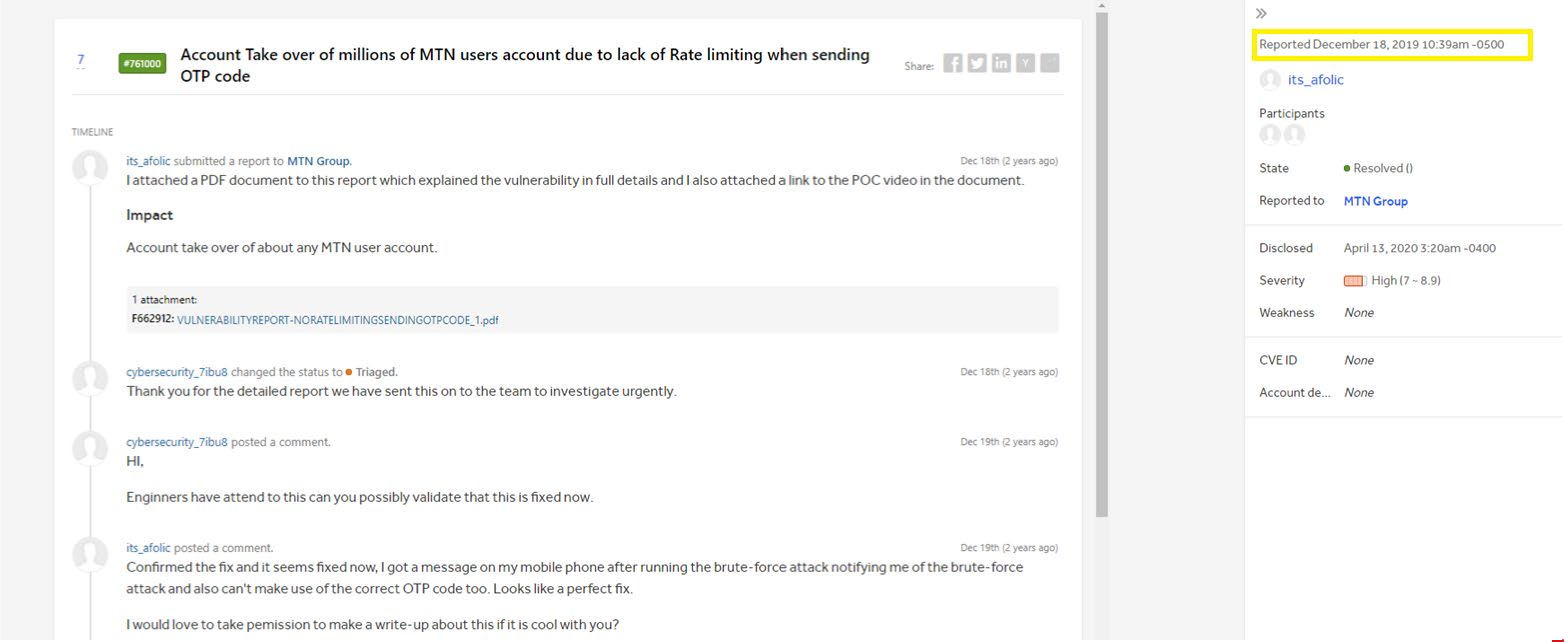
Assets in scope
28

Submit report

Vulnerability Disclosure Program

Launched on Dec 2019

Private disclosures enabled



7 #761000 **Account Take over of millions of MTN users account due to lack of Rate limiting when sending OTP code**

Share:

TIMELINE

its_afolic submitted a report to MTN Group. — Dec 18th (2 years ago)

I attached a PDF document to this report which explained the vulnerability in full details and I also attached a link to the POC video in the document.

Impact

Account take over of about any MTN user account.

1 attachment:
F662912: VULNERABILITYREPORT-NORATELIMITINGSENDINGOTPCODE_1.pdf

cybersecurity_7ibu8 changed the status to ● Triaged. — Dec 18th (2 years ago)

Thank you for the detailed report we have sent this on to the team to investigate urgently.

cybersecurity_7ibu8 posted a comment. — Dec 19th (2 years ago)

HI,

Enginners have attend to this can you possibly validate that this is fixed now.

its_afolic posted a comment. — Dec 19th (2 years ago)

Confirmed the fix and it seems fixed now, I got a message on my mobile phone after running the brute-force attack notifying me of the brute-force attack and also can't make use of the correct OTP code too. Looks like a perfect fix.

I would love to take pemission to make a write-up about this if it is cool with you?

Reported December 18, 2019 10:39am -0500

its_afolic

Participants

State	● Resolved ()
Reported to	MTN Group
Disclosed	April 13, 2020 3:20am -0400
Severity	High (7 ~ 8.9)
Weakness	*None*
CVE ID	*None*
Account de...	*None*

[2]

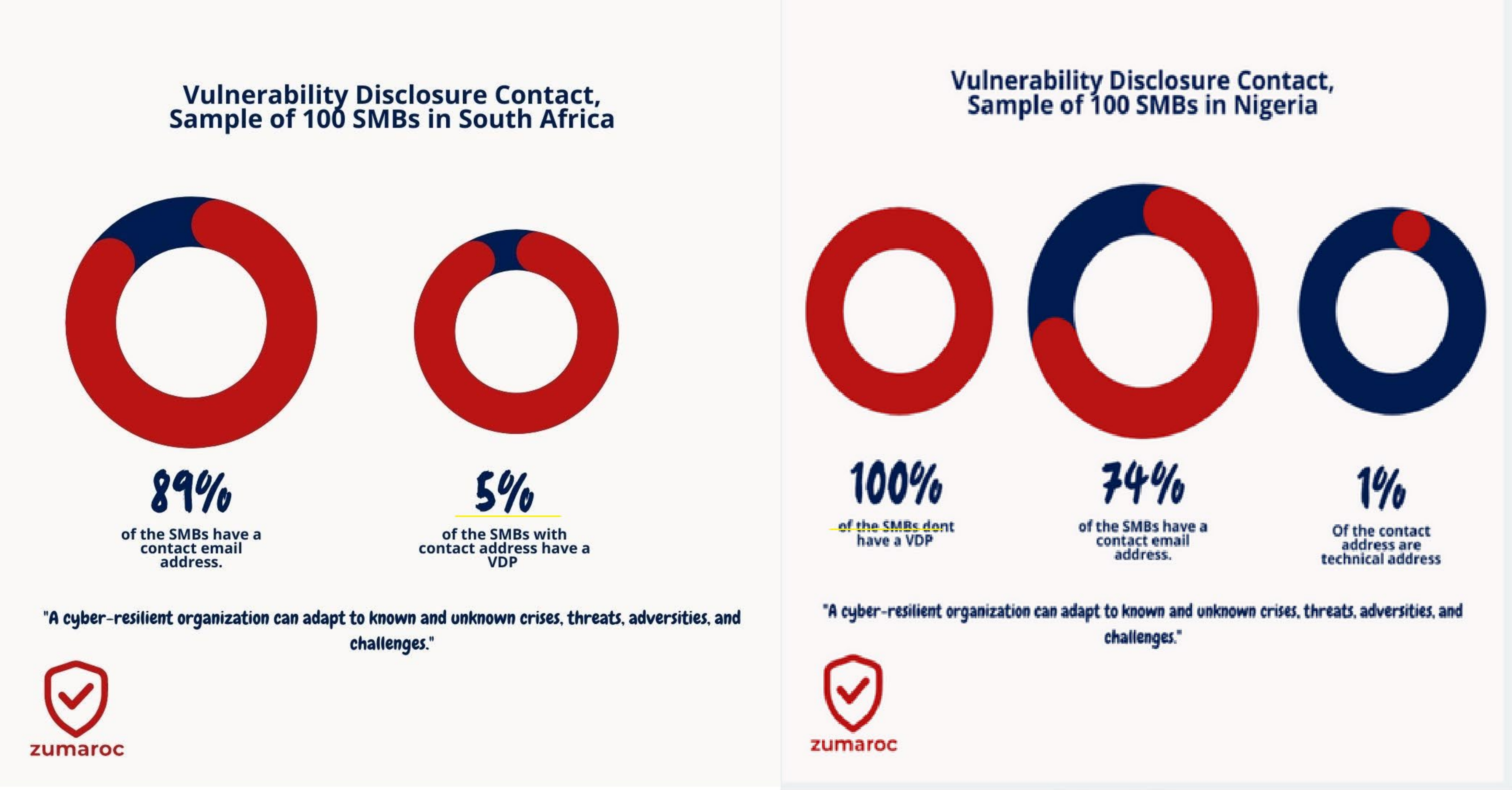
Zumaroc

3b. The impact of security research – Zumaroc

3 min

Cyber Resilience Index | Africa 2021 Report

- Researchers have created an **Index that measures the cyber resilience** of companies in Africa
- A firm follows cyber resilience methodologies by having a **public or private** Vulnerability Disclosure Program (VDP).



Vulnerability Disclosure Contact, Sample of 100 SMBs in South Africa

"A cyber-resilient organization can adapt to known and unknown crises, threats, adversities, and challenges."

zumaroc

Vulnerability Disclosure Contact, Sample of 100 SMBs in Nigeria

"A cyber-resilient organization can adapt to known and unknown crises, threats, adversities, and challenges."

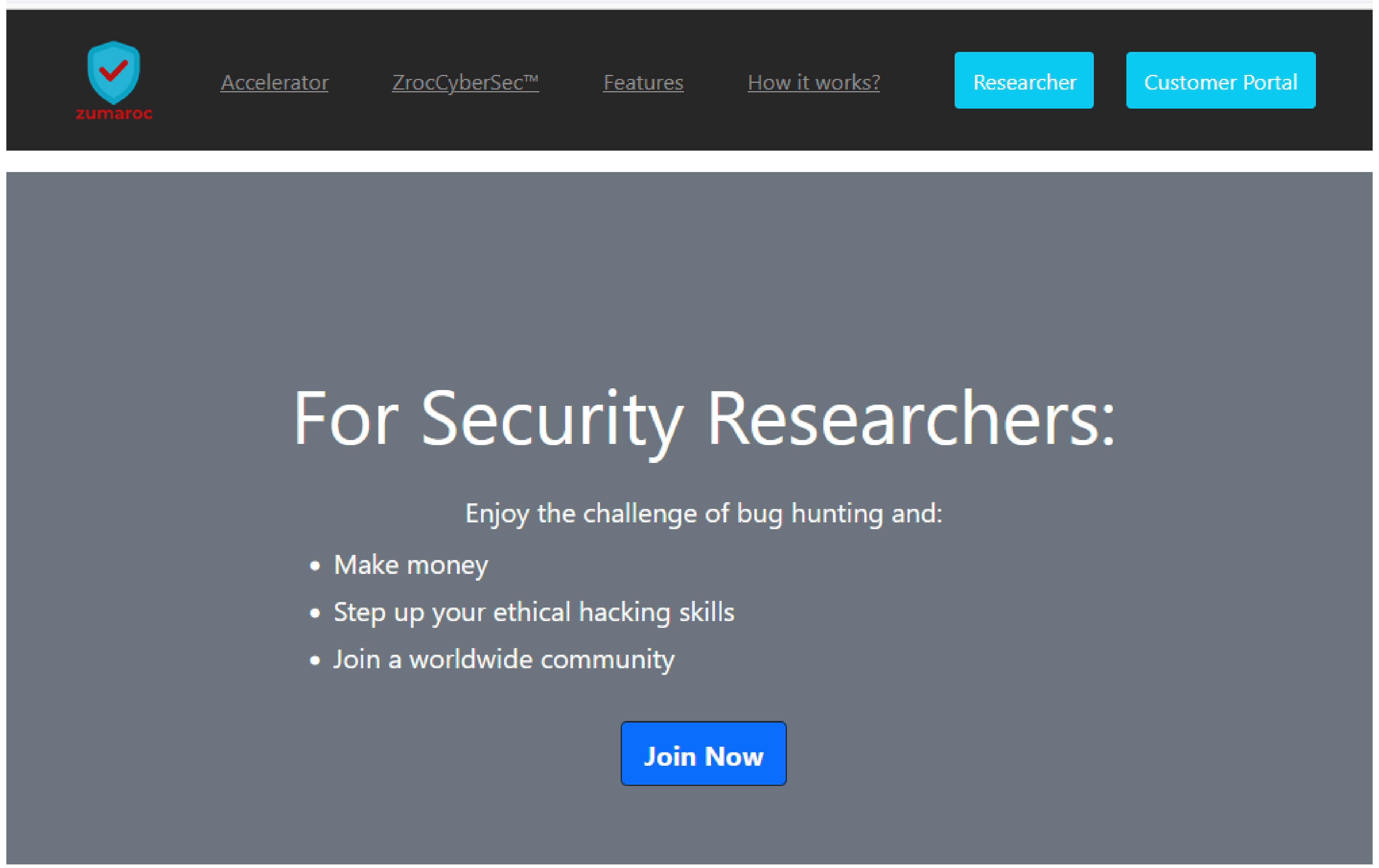
zumaroc

4. How do you Get Started ?

3 min

Security Researcher?

Join an **online community**.



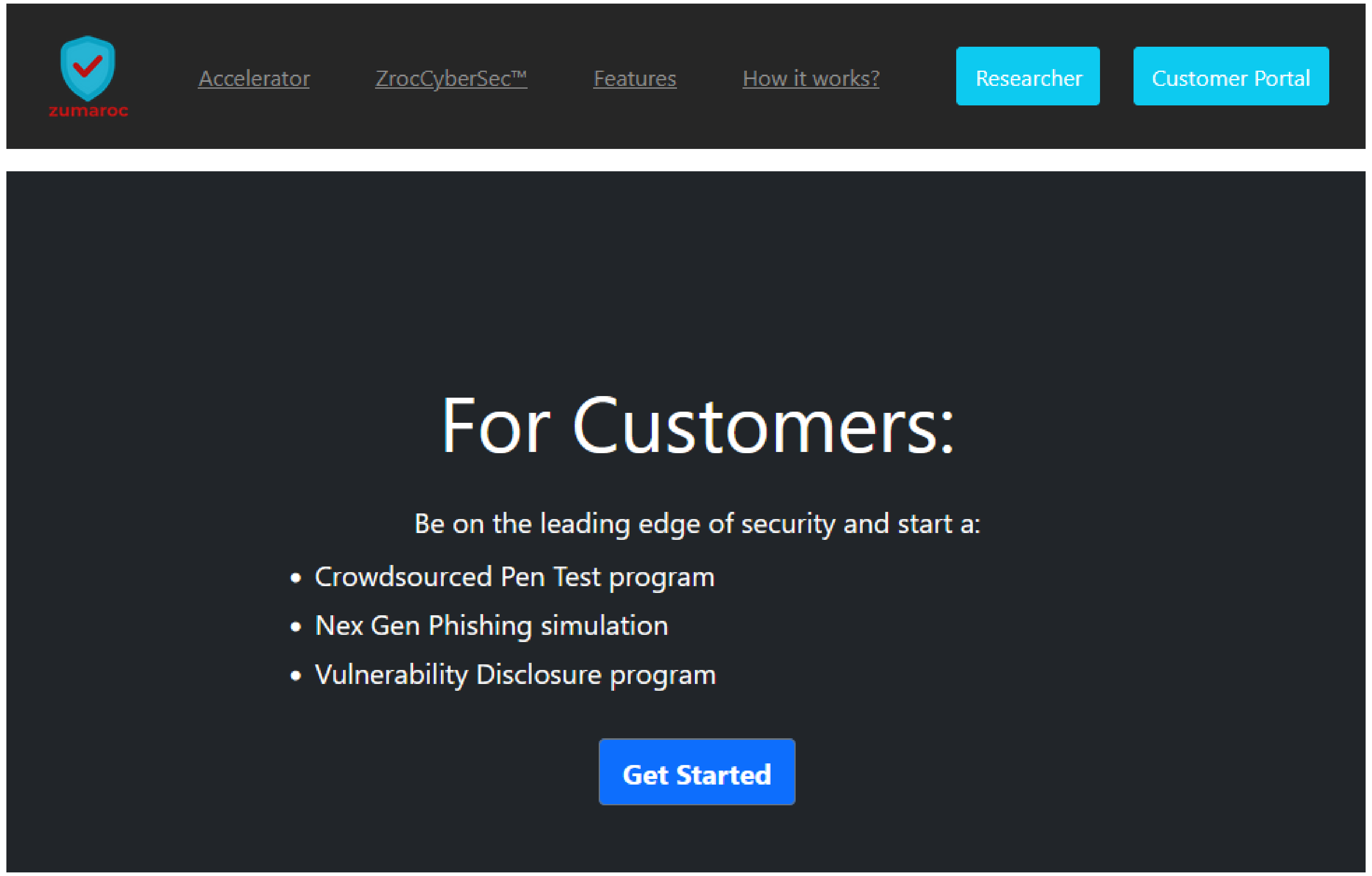
For Security Researchers:

Enjoy the challenge of bug hunting and:

- Make money
- Step up your ethical hacking skills
- Join a worldwide community

Company?

Engage the **online community**.



For Customers:

Be on the leading edge of security and start a:

- Crowdsourced Pen Test program
- Nex Gen Phishing simulation
- Vulnerability Disclosure program

Zumaroc

5. Questions & Answers

5 min

Common Questions:

- *What is a **Bug**?*
- *What are some of the **challenges** of becoming an ethical hacker?*
- *How **safe** is using crowdsourced security at my organization?*

Further activities

- **Email zroc@zumaroc.com for a copy of Cyber Resilience Index | Africa**

Zumaroc