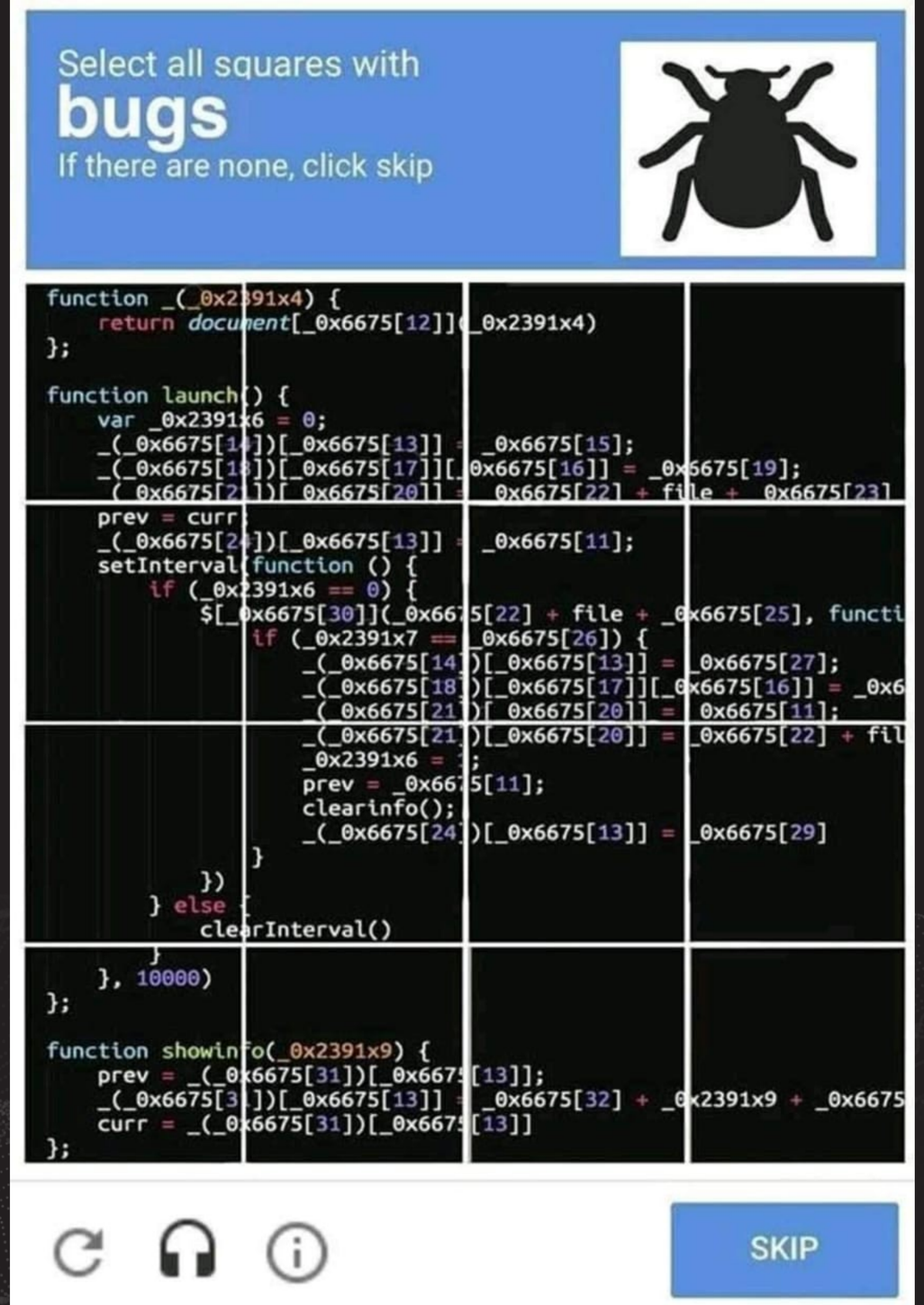
Vamos caçar bugs?!

Anchises Moraes | Cyber Evangelista

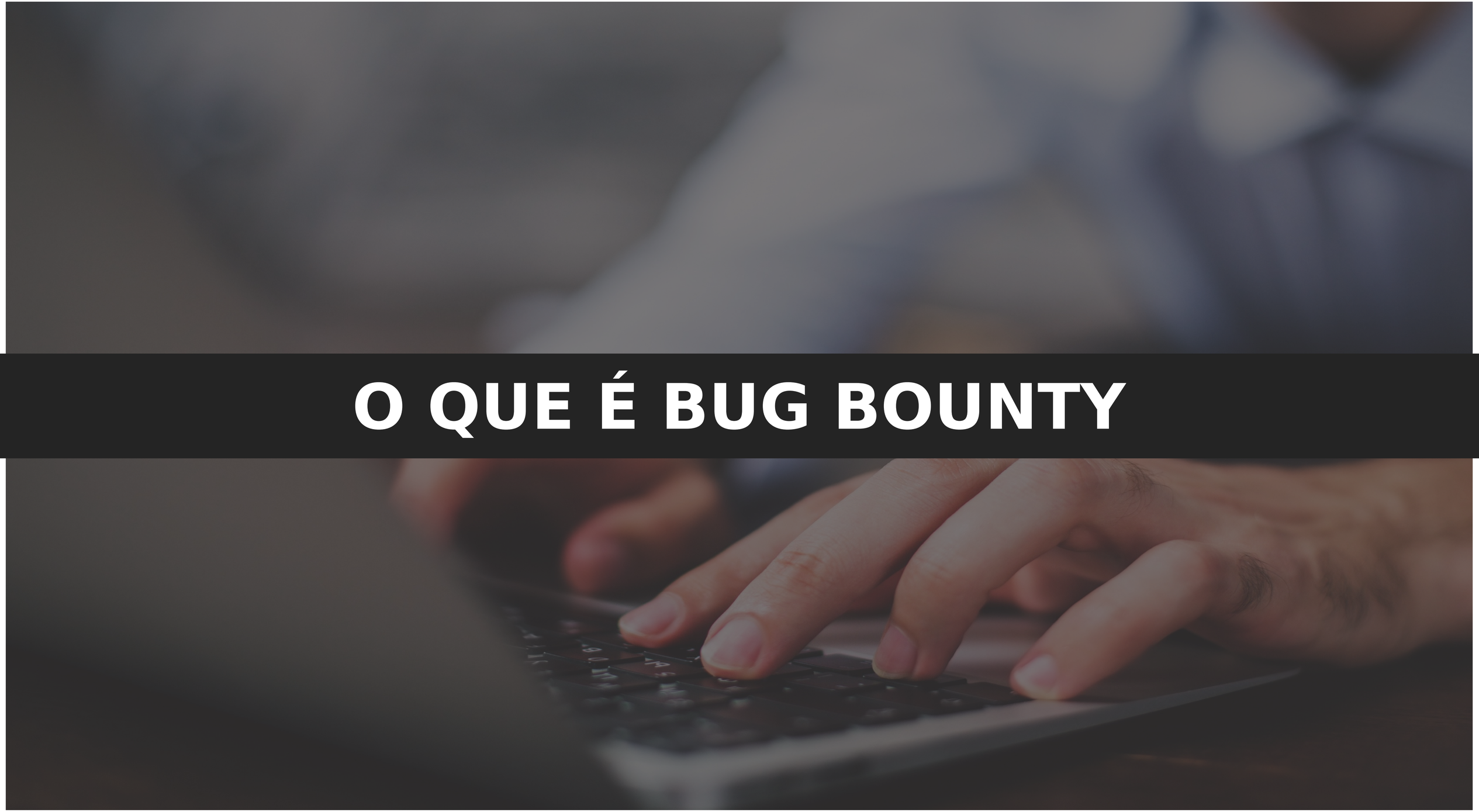
AGENDA

O que é Bug Bounty

Desafios e Lições aprendidas



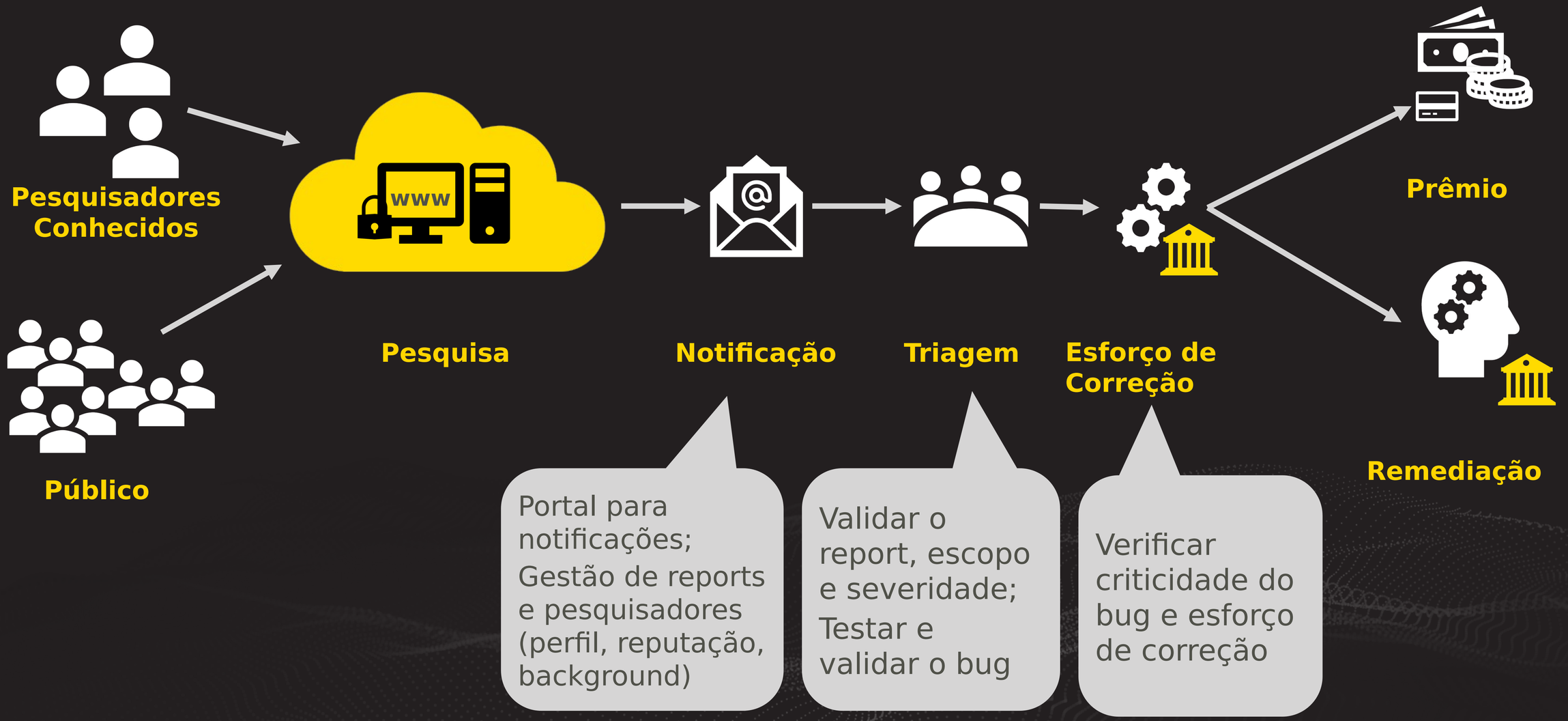
C6BANK



O QUE É BUG BOUNTY

VULNERABILITY DISCLOSURE
Canal para receber notificações de vulnerabilidades

BUG BOUNTY
Recompensa para quem reportar problemas de segurança


Pesquisadores
Conhecidos
Público
www
Pesquisa
Notificação
Triagem
Esforço de
Correção
Prêmio
Remediação
Portal para notificações;
Gestão de reports e pesquisadores (perfil, reputação, background)
Validar o report, escopo e severidade;
Testar e validar o bug
Verificar criticidade do bug e esforço de correção

VANTAGENS PARA OS PESQUISADORES

Ganho financeiro

VANTAGENS PARA OS PESQUISADORES

August 30th, 2019

threatpost

Six Hackers Have Now Pocketed $1M From Bug Bounty Programs

https://threatpost.com/six-hackers-1m-bug-bounty-programs

C6BANK

VANTAGENS PARA OS PESQUISADORES

Ganho financeiro

Oportunidade de estudo

VANTAGENS PARA OS PESQUISADORES

Ganho financeiro

Oportunidade de estudo

Pesquisa ética

C6BANK

VANTAGENS PARA AS EMPRESAS

C6BANK

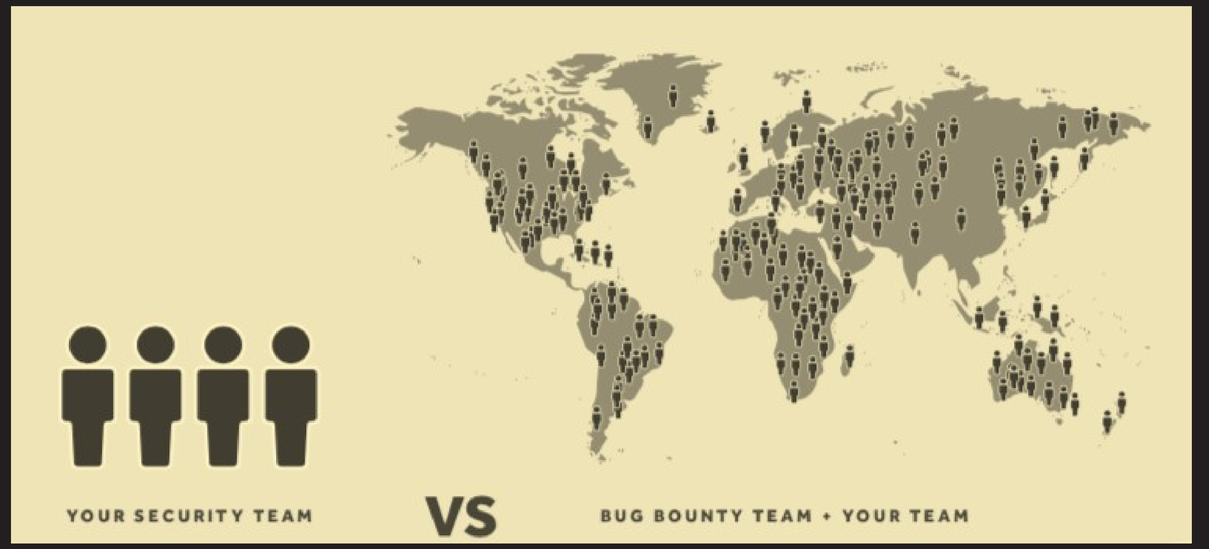
Identificar bugs

VANTAGENS PARA AS EMPRESAS

VANTAGENS PARA AS EMPRESAS

Identificar bugs

Diversidade



- Estudo “An Empirical Study of Vulnerability Rewards Programs” (Berkeley)
  - An increase in the number of researchers looking for vulnerabilities yields an increase in the diversity of vulnerabilities discovered.

VANTAGENS PARA AS EMPRESAS

Identificar bugs

Diversidade

Custo x Benefício

- Estudo “An Empirical Study of Vulnerability Rewards Programs” (Berkeley)
  - A Vulnerability Research Program (VRP) can be a **cost-effective** mechanism for finding security vulnerabilities.
  - The cost of (...) VRPs is comparable to the cost of just **one member** of the browser security team.
  - Each of these VRPs finds **many more vulnerabilities than any one researcher** is likely to be able to find.

https://mfinifter.github.io/papers/vrps-usenix2013.pdf

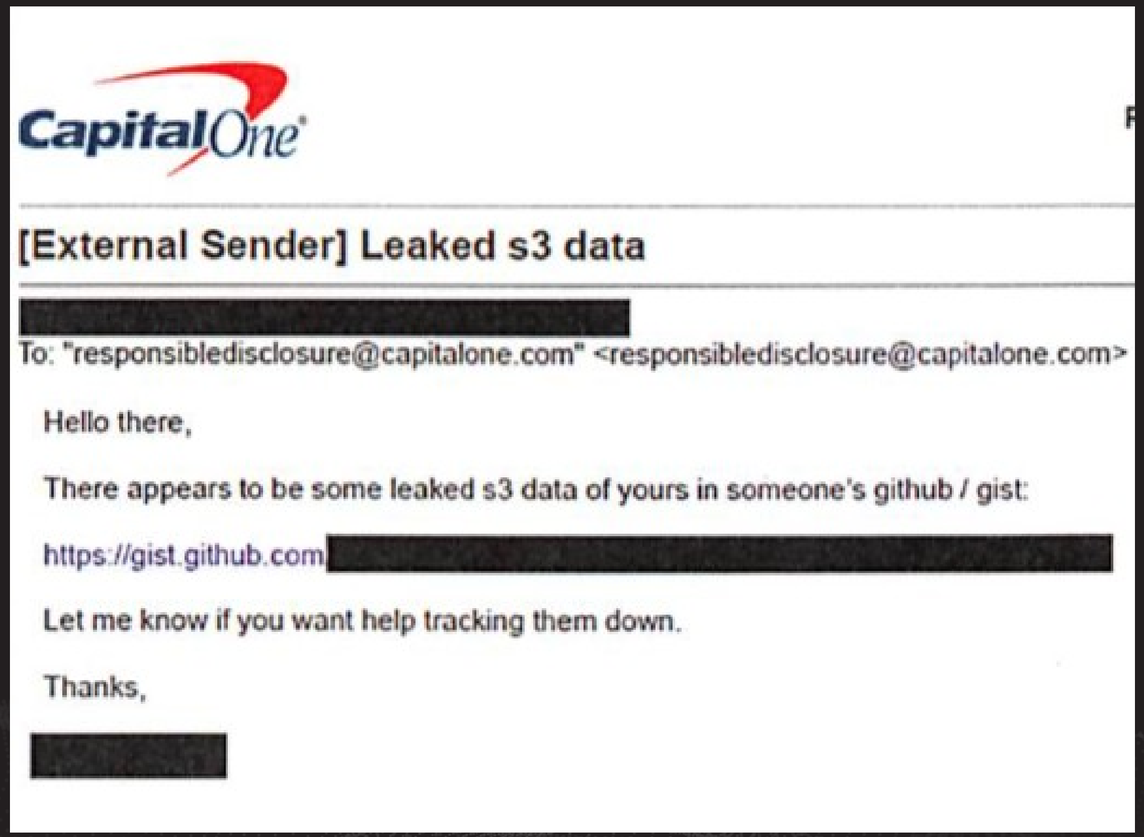
VANTAGENS PARA AS EMPRESAS

Identificar bugs

Diversidade

Custo x Benefício

Canal de notificações



[External Sender] Leaked s3 data

[redacted]

To: "responsibledisclosure@capitalone.com" <responsibledisclosure@capitalone.com>

Hello there,

There appears to be some leaked s3 data of yours in someone's github / gist:

https://gist.github.com[redacted]

Let me know if you want help tracking them down.

Thanks,

[redacted]

Fonte: www.justice.gov

DESAFIOS

C6 Bank

Apr 24 · 3 min read

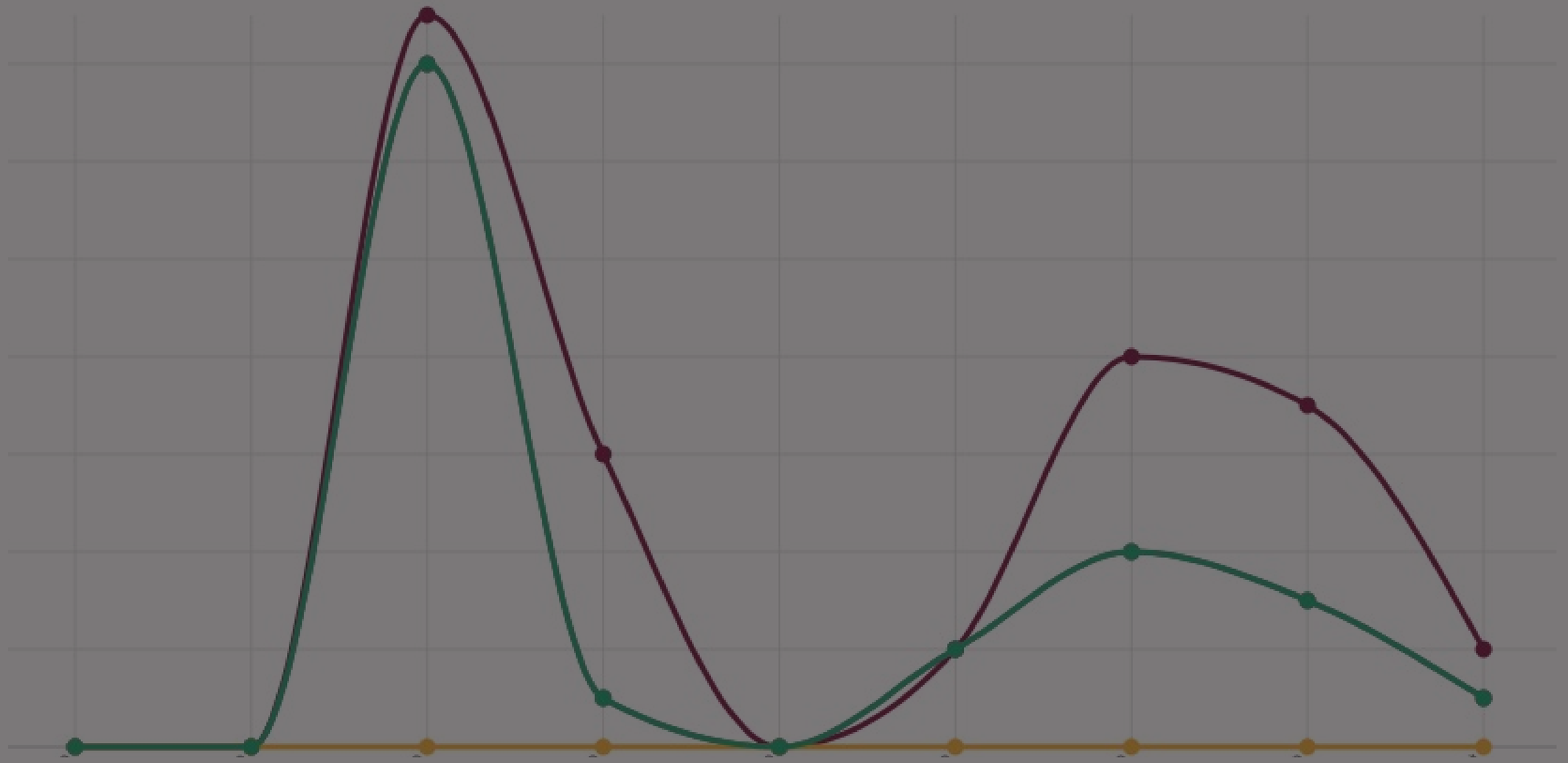
C6 Bank lança programa de "bug bounty"

Iniciativa é uma parceria do banco com a HackerOne, maior comunidade de pesquisadores de…

Read more…

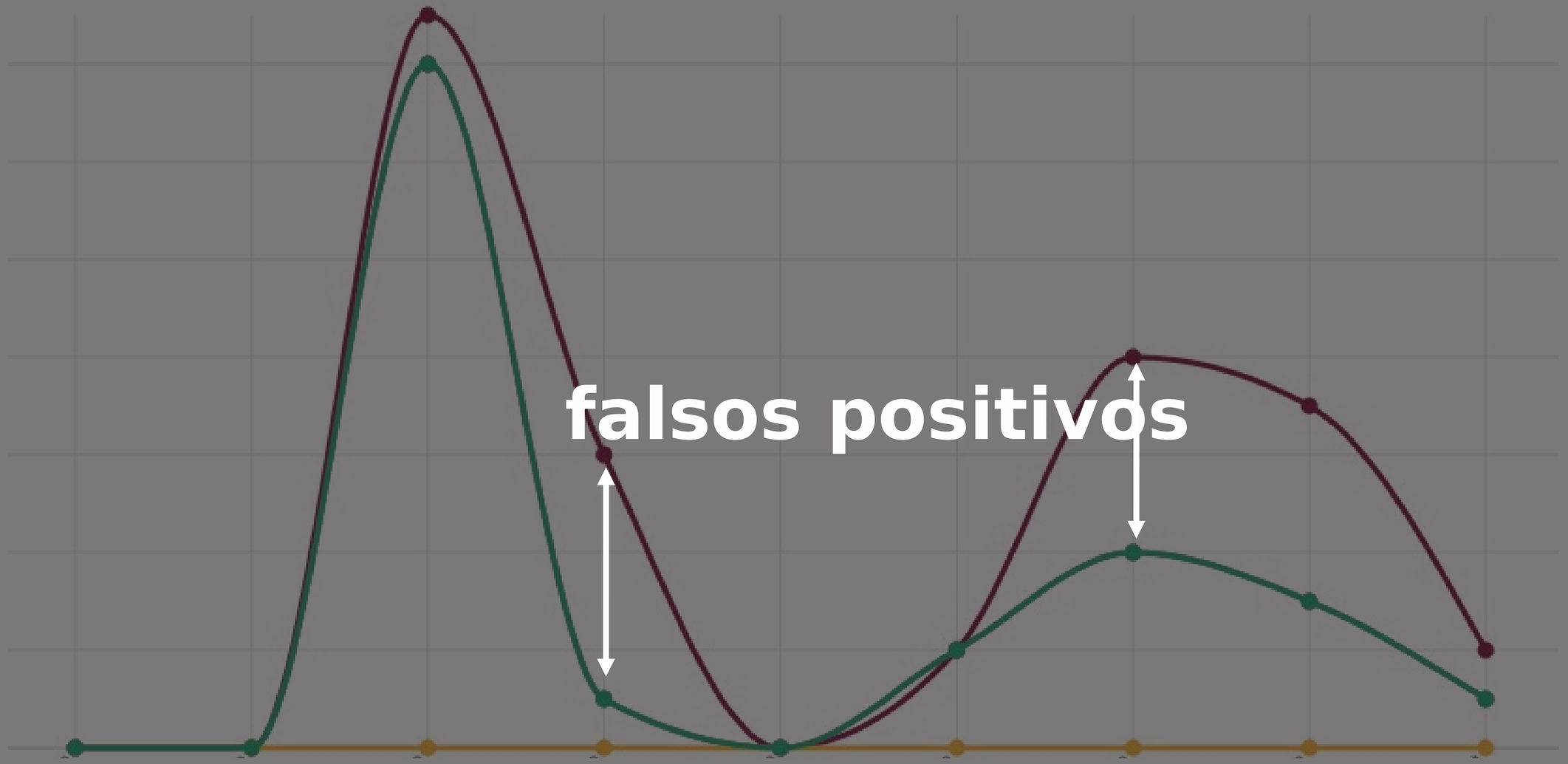
https://medium.com/@C6bank/c6-bank-lan%C3%A7a-programa-de-bug-bounty-1f419ebec9f2

C6BANK



Classificação:

Classificação:



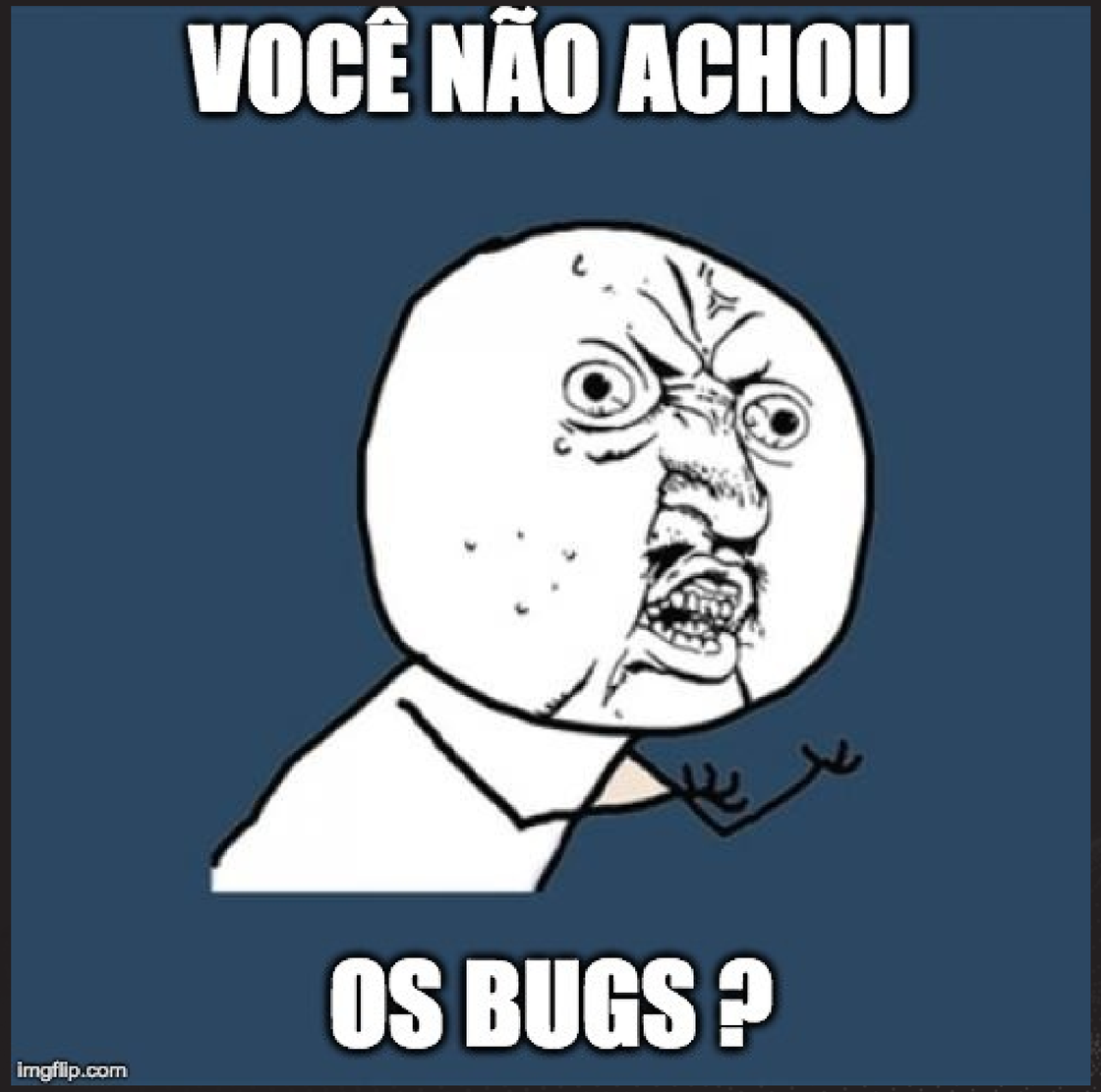
Classificação:

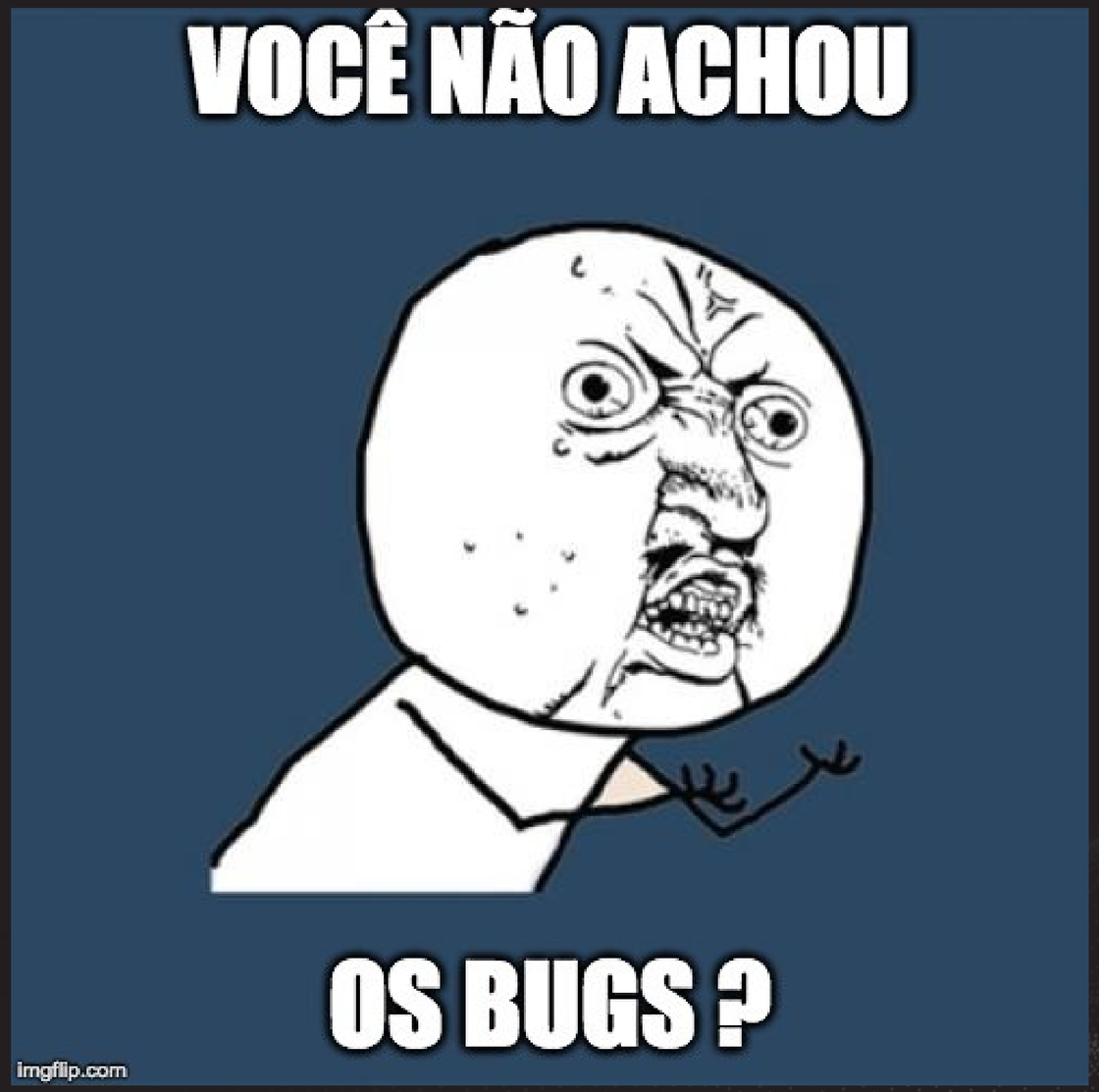
PROCESSO DE RESPOSTA

Velocidade (SLA)

Retorno / recompensa

Correção


VOCÊ NÃO ACHOU
OS BUGS ?
imgflip.com



“Testing only proves the presence of bugs, not the absence of them.”

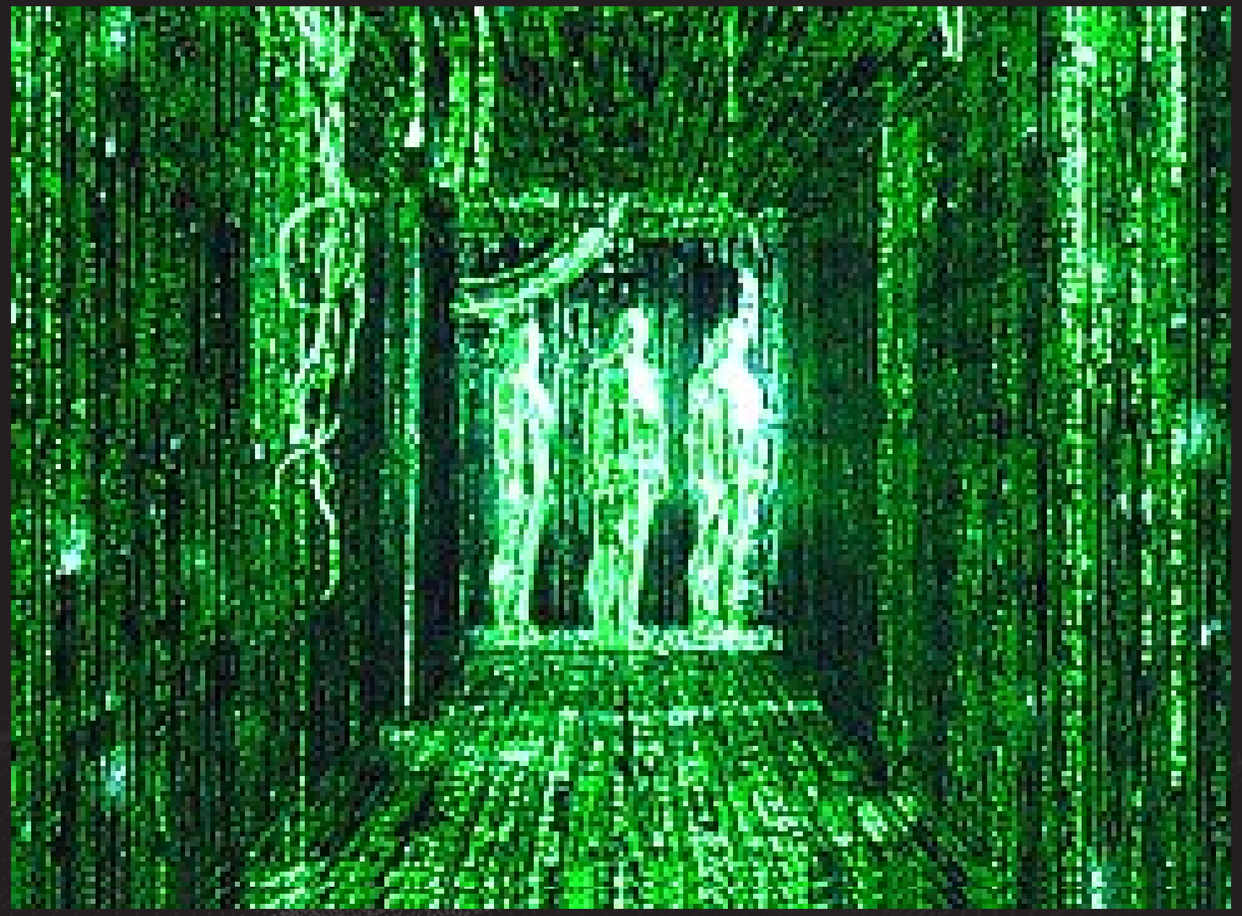
Louis Cremen

https://hackernoon.com/introducing-the-infosec-colour-wheel-blending-developers-with-red-and-blue-security-teams-6437c1a07700

LIÇÕES APRENDIDAS

TESTAR NOVOS CENÁRIOS

Ex. “Blind SQL Injection”



MÉTRICA PARA MEDIR O CUSTO DOS BUGS

	Bounty Table / Rewards (Best case)			
Empresa	**Crítical**	**High**	**Medium**	**Low**
Robinhood	$ 50.000	vários	vários	$ 100
Coinbase	$ 50.000	$ 15.000	$ 2.000	$ 200
Paypal	$ 20.000	$ 10.000	$ 1.000	$ 100
Goldman Sachs	$ 15.000	vários	vários	$ 250
QIWI	$ 5.000	$ 5.000	$ 500	$ 200
Credit Karma	$ 5.000	$ 2.250	$ 700	$ 250
Savedroid	$ 2.500	$ 1.500	$ 500	$ 250
	$	$	$	$

Fonte: Hackerone

C6BANK

OBRIGADO

Anchises Moraes | Cyber Evangelista
anchises.moraes@c6bank.com

C6BANK

https://www.c6bank.com.br