

# Bug Bounty @Telenet

The Hitchhiker's Guide to Bug Bounty



Bruno De Legher

16-06-2022



# Who Am I?

**Bruno De Legher**

17+ years @Telenet

7+ years Security Officer

Cyber Security Coalition member since 2011 (CSIRT)

Bug Bounty program owner

Focus on governance, awareness, customer security and security by design in an Agile environment



# Telenet in a nutshell

€  
**2,5  
billion  
revenue**



**Headquarters  
Mechelen**



**3.600  
Employees**



**± 2 million  
television  
customers**



**+ 2,8  
million  
mobile  
customers**

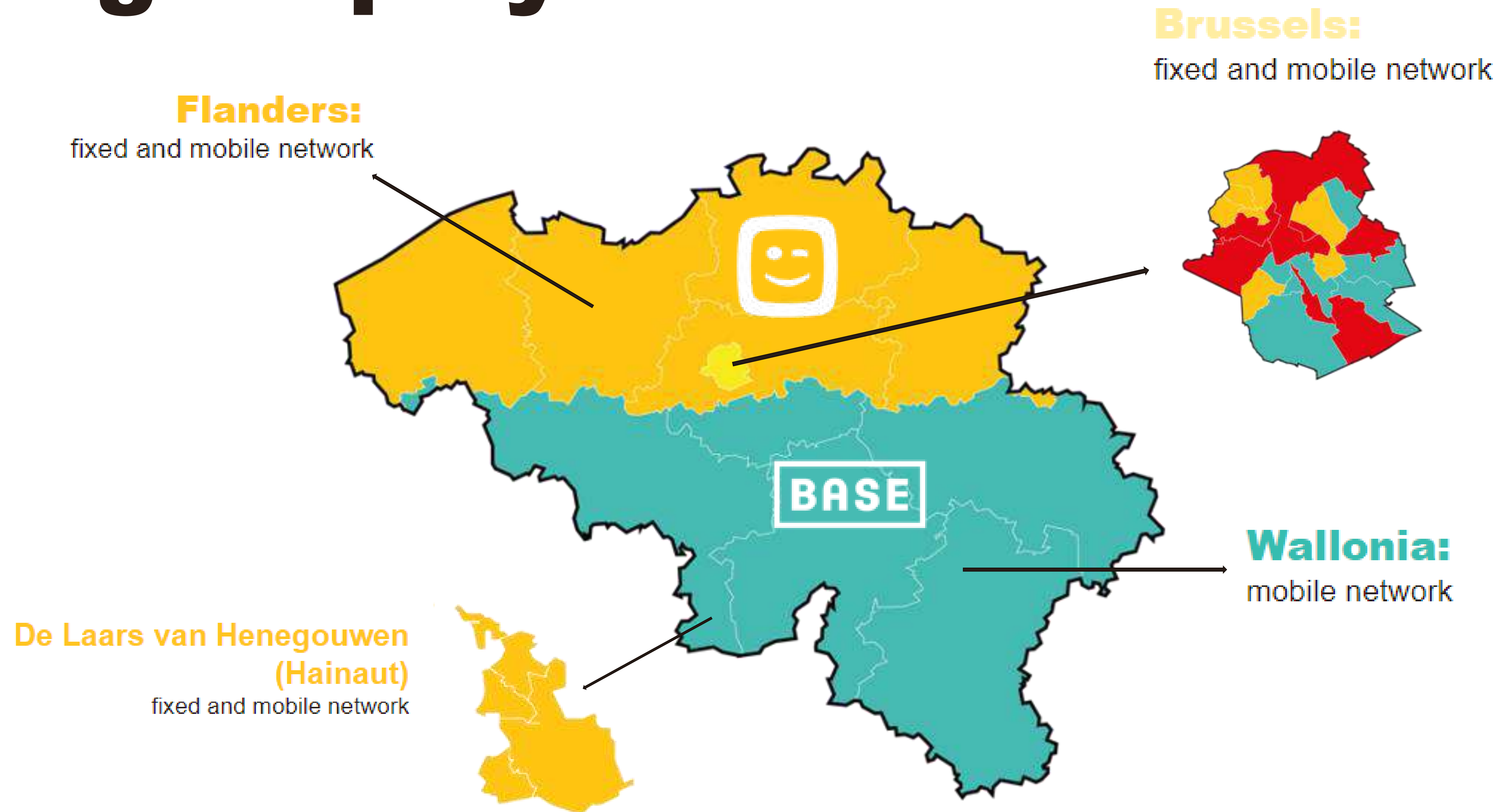


**+ 1,6  
million  
broadband  
internet  
customers**





# Belgian player





# Media & entertainment with local presence



PLAY **1.**  
PLAY **5**

PLAY **6**  
PLAY **7**

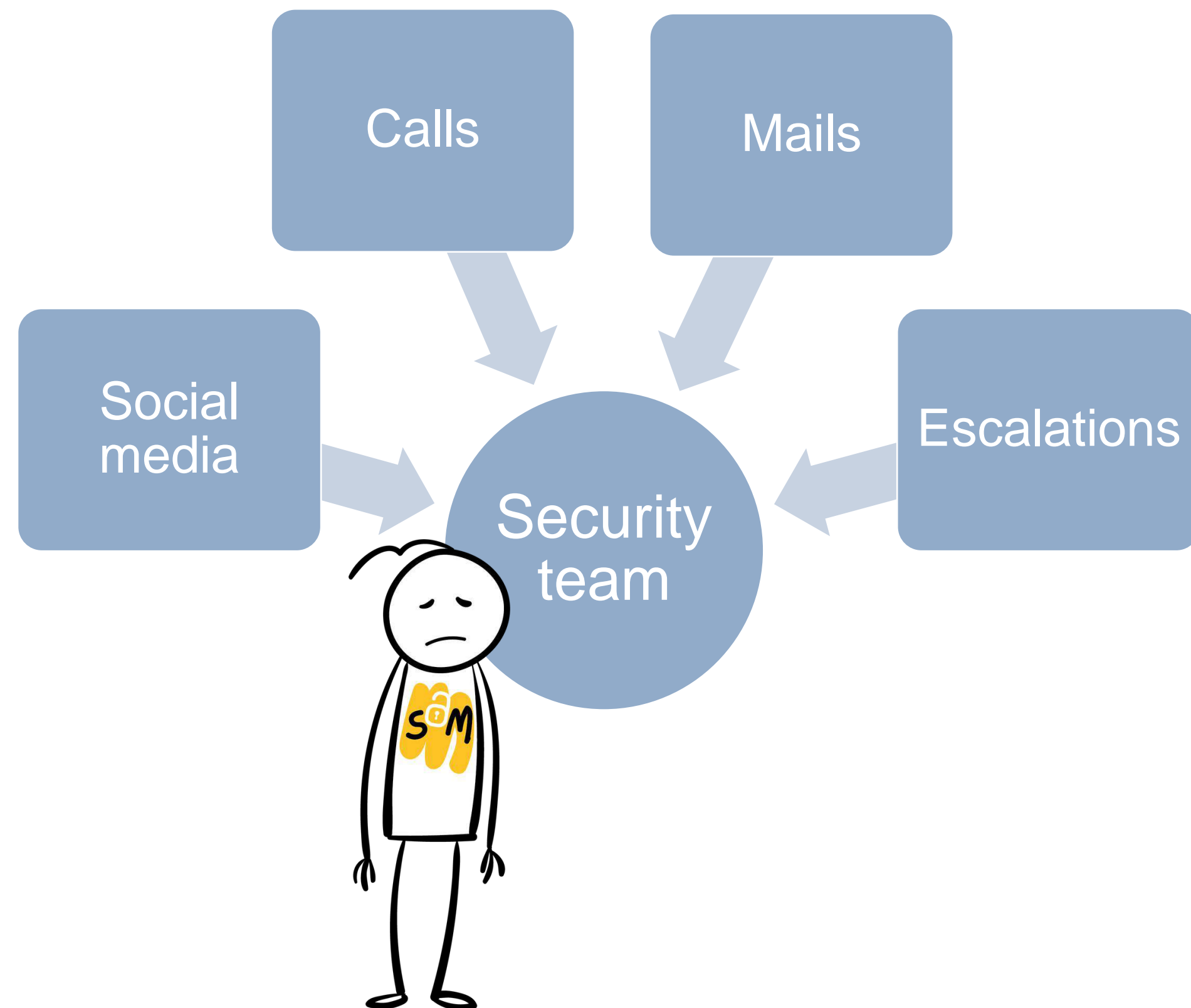


**CAVIAR**

**Ads & Data**  
*We un-waste*



# Bug Bounty: How it all began?





# Responsible Disclosure

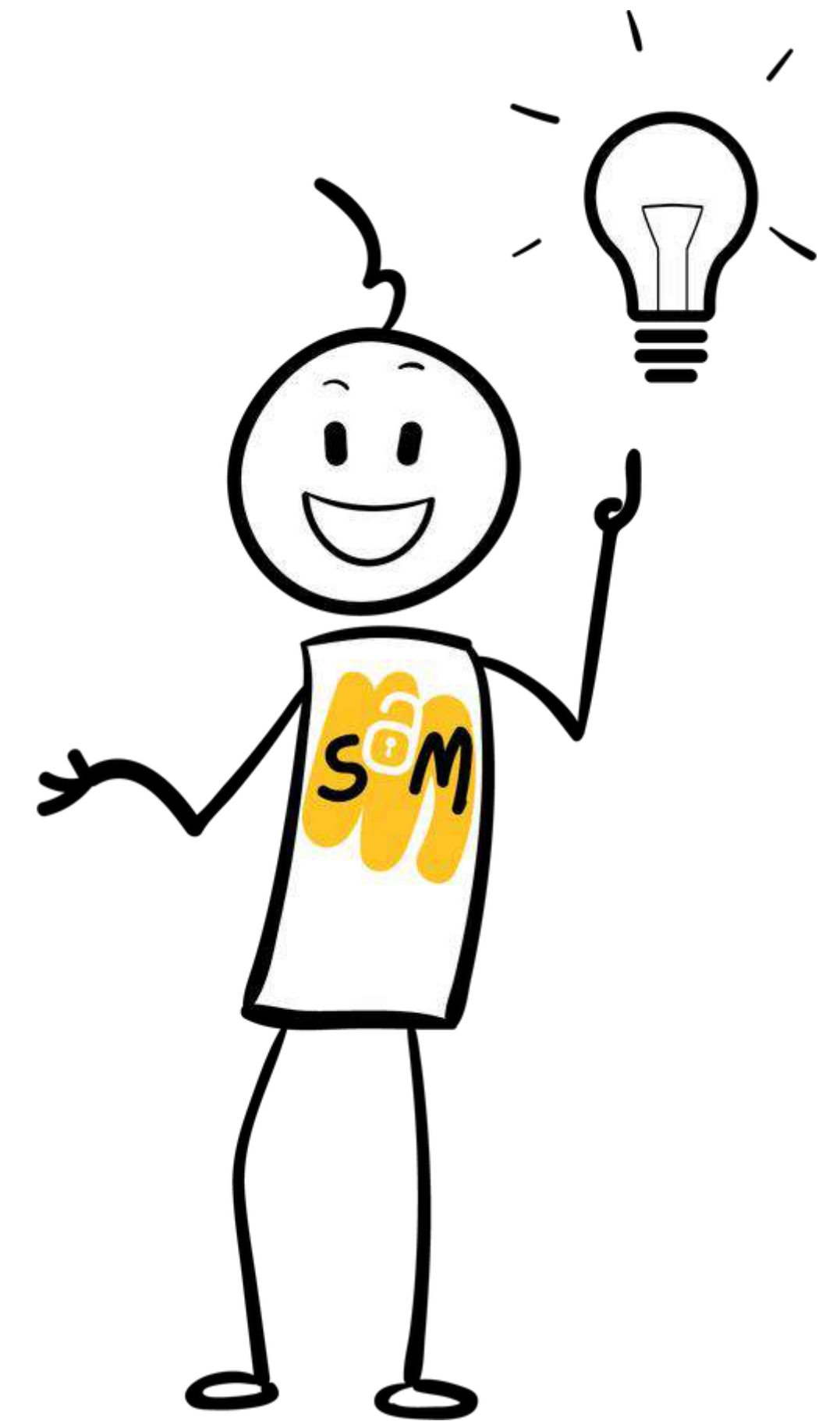
2015

**Published responsible disclosure policy (PDF)**

**Published reporting form on Telenet.be website**

**But... it has limitations...**

- **Manual follow-up via mail**
- **95% of inflow was meant for customer care**
- **Duplicates**
- **No triage**
- **Exceptional gift/bounty process was complex**



# Intigriti @Telenet

**2018** – Moved Responsible Disclosure to Intigriti

**2019** – Added BASE brand to the Telenet RD program

**2019** – Invite only Bug Bounty program for Base & Telenet

**2020** – Bug Bounty program for Base & Telenet

## Future plans...

Increase scope, onboard new brands & ventures





# Our program scope

<https://app.intigriti.com/programs/telenet/telenetgroup/detail>



## Out of scope

Leaked customer credentials or customer abuse, please contact our abuse team via [abuse@telenet.be](mailto:abuse@telenet.be)

Services and systems that are hosted, created, managed or owned by Telenet customers.

## FAQ

### **Can we receive test accounts?**

No, we currently don't share credentials of test accounts.

### **How long does it take to fix a vulnerability?**

Our goal is to implement a fix as soon as possible. Depending on the criticality and the affected system it can take up to multiple months to implement a fix.

### **Why have you lowered the criticality of my reported issue?**

If the reported issue has been found on a non-critical system or non-production environment then we can downgrade the criticality.

In this program we try to focus on critical and production environments.

### **Do you give refunds for Telenet services I have bought for testing purposes.**

We do not recommend to buy Telenet services for testing purposes.

Expenses for services you have bought for testing purposes cannot be refunded. Sales are final.



# Tips & Tricks

## Keep security researchers happy!

- Communicate
- Give bonuses
- Bug Bounty programs do not replace penetration testing, code review or vulnerability scanning
- Start with a small scope or invitation/RD program.
- Accept bounties for shadow-IT & lower environments (to some extend)
- Update scope and bounties regularly
- Use invitation only function for beta testing
- Accept the risk that there is always a risk that an ethical hacker can break something
- Build a FAQ





# Questions?





**Thank**  
**You!**





