

# Welcome!

How ethical hackers help us improve security in Visma



**Ioana Pirooska**

Bug Bounty Program Manager

# Agenda



- 🛡️ Visma & VSP

- 🛡️ Hacking and hackers

- 🛡️ Bug Bounty and RD

- 🛡️ Common vulnerabilities, critical bugs & exceptional people

- 🛡️ Some program stats and payouts

- 🛡️ Key takeaways

- 🛡️ Useful links/how to get started

# Visma in short



**Leading cloud products in Europe**



**Develop and deliver software**  
small businesses, medium and  
large enterprises & public sector



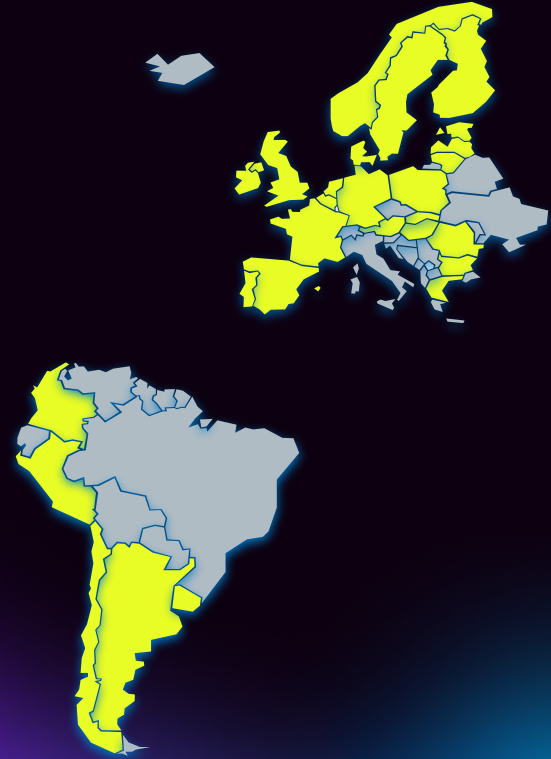
**Wide network**  
of distributors and partners



**Large and diversified**  
technology stack



Operate across Europe and  
Latin America



# Visma in numbers



**15.300+**

Engaged employees



**1.7M**

Customers



**€ 2 392M**

Total Revenue  
Value created for **society**



**5000+**

Developers



**265+**

Locations - strong local presence  
**We are where you are**



**11M & 23M**

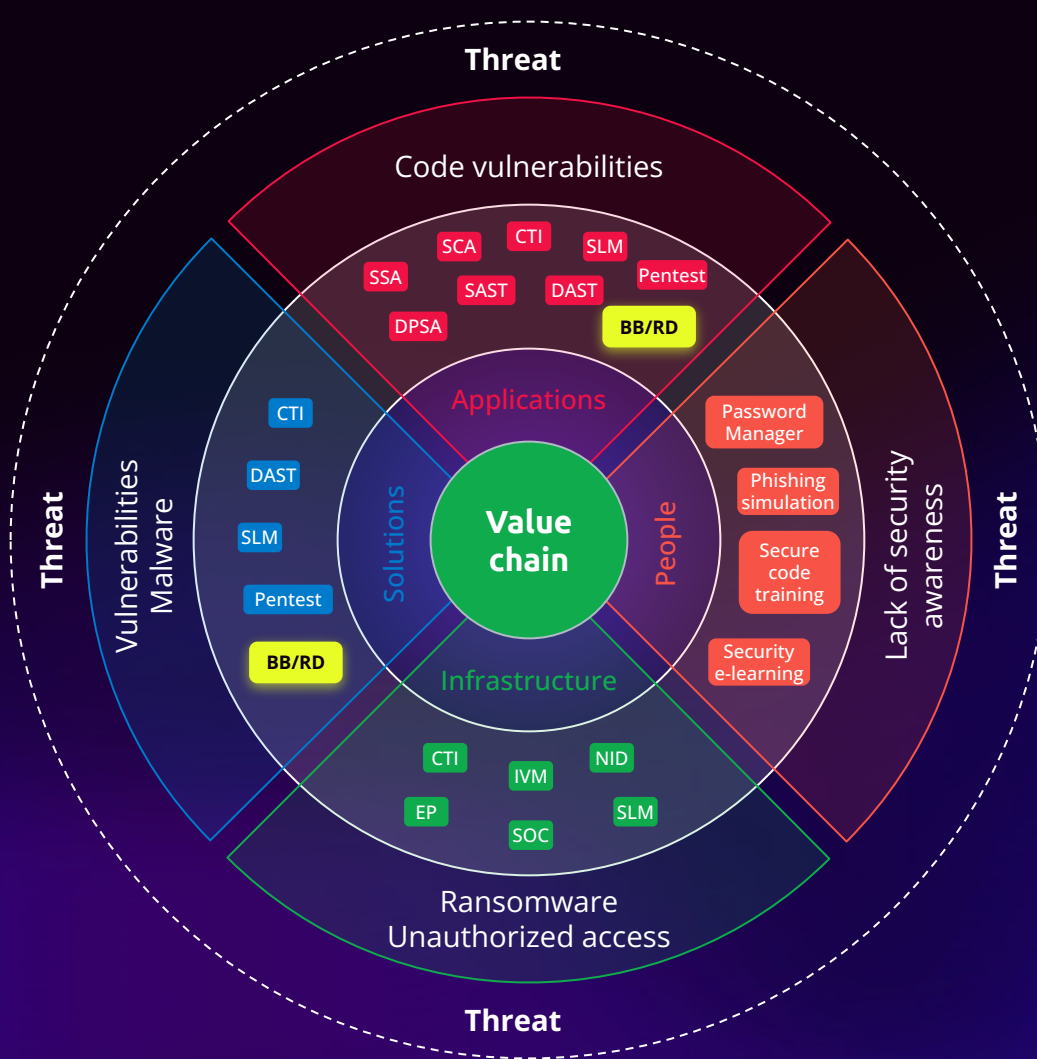
Payslips e-invoices  
running through Visma's systems  
every month



**300**

Companies have joined Visma  
last decade





# Hacking and hackers

## White hats

Ethical hackers/security researchers  
with genuine desire of improving  
information security

Explicit permission from the owner

Motivated by learn something new, gain  
MONEY in an ethical way

## Gray hats

may violate ethical standards or  
principles

without malicious intent

Often juniors - Script Kiddies

Use tools or scripts developed  
by others to perform their hacks

Motivated by "making the world  
safer", learn something new,  
MONEY

## Black hats

Cyber criminals/malicious intent

Create malware

Criminal organizations

State sponsored/Hacktivists/Suicide  
hackers

Motivated by MONEY, religious or  
political beliefs



# What is Bug Bounty?



Hackers with specialized skills



Legal Permission to hack  
*(respect policies, rules and do not do harm)*



Power of the crowd



Continuously testing the applications for \$\$\$

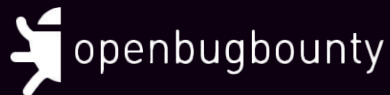


More researchers = More findings = Better security

# Platforms & tools

## Platforms

hackerone



YES WE H/CK

bugcrowd



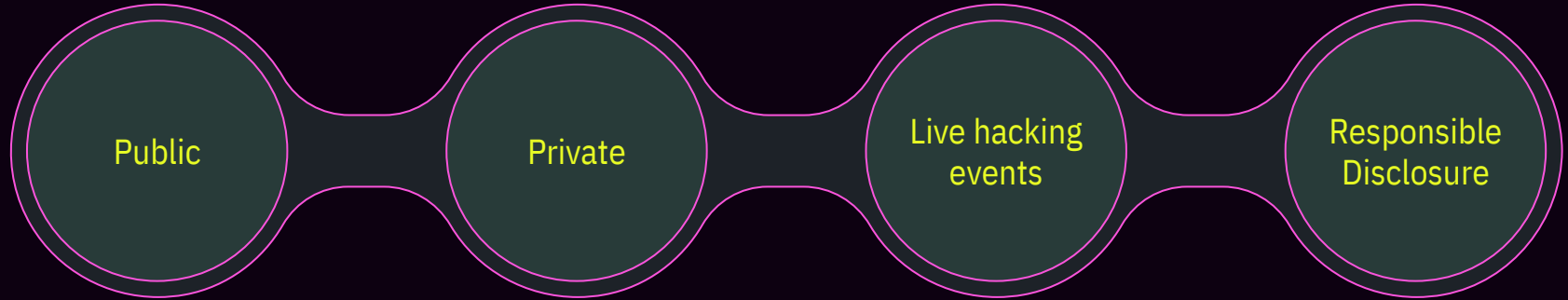
INTIGRITI


## Tools






# Program Types




 Hundreds of thousands of hackers - entire community


 Self sign in


 Less domains in scope


 Invite only program


 Very good quality


 Many domains in scope


 Exclusive events with a pool of hackers invited

 A more restricted scope

 **2 weeks** of live hacking virtual/physical

 Public for the entire community

 All Visma assets are in scope

 No bounties, just swags and HOF

**360+** submissions and **€90K** spent

**700+** submissions and **194K** spent

# Why Responsible Disclosure

Published and hosted through BB platform: [Visma Responsible Disclosure](#)

Self published: [RD Visma Trust Centre](#)

[Visma Swag Store](#)

[Visma Security Hall of Fame](#)

All time stats



**1100+**

Fixed reports



**91**

Criticals

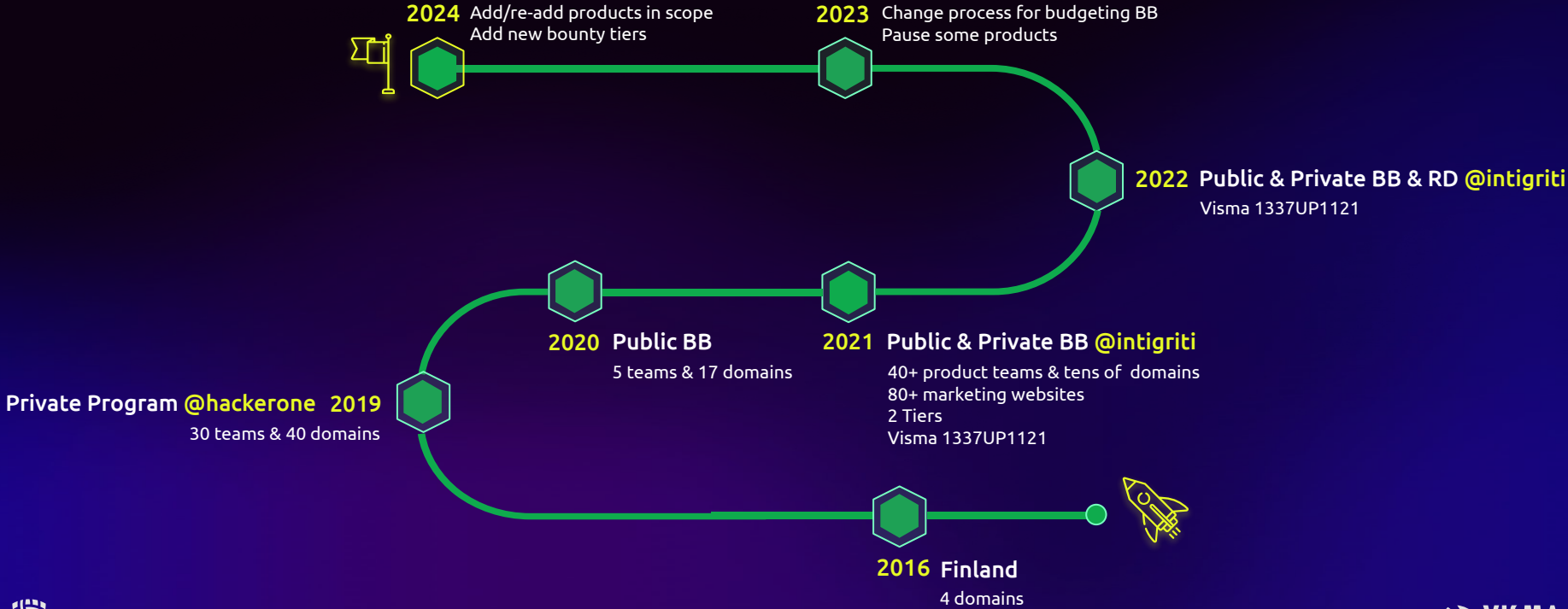


**260+**

Researchers on HOF



# Bug Bounty journey



# Ready for Bug Bounty?

Internal pentest < 12 months  
1 pentest done on the BB environment or similar

SAST (Polaris or Coverity)

SCA (Aikido)

DAST (Detectify)

RD

Zero known vulnerabilities



Environment

Test accounts

Test data

Documentation

Commitment

Validate bugs in **2-4 business days**

Fix critical bugs within **5 days**

Fix within **90 days**

# Work smart - use automation



## Credentials management

<https://github.com/visma-prodsec/BugBountySelfServicePortal>

### Admin

- See the number of unclaimed credentials for each service
- View credentials for all services and hackers
- Add a new service & import a set of credentials from a CSV

### Hacker

- See all available services
- See all your assigned sets of credentials
- Claim new credentials



## Intigriti - Jira integration

Reports pushed automatically from Intigriti to Jira



## Tool for stats

Costs/Team, Top 10 bug types, Resolution times

# Bug Bounty vulnerabilities

Top submission types

**Information Disclosure**

8.6%

**Improper Authorization**

9.1%

**Improper Access Control**

16.8%

**Insecure Direct Object Reference**

8.0%

**Privilege Escalation**

10.8%

**Reflected Cross-Site Scripting**

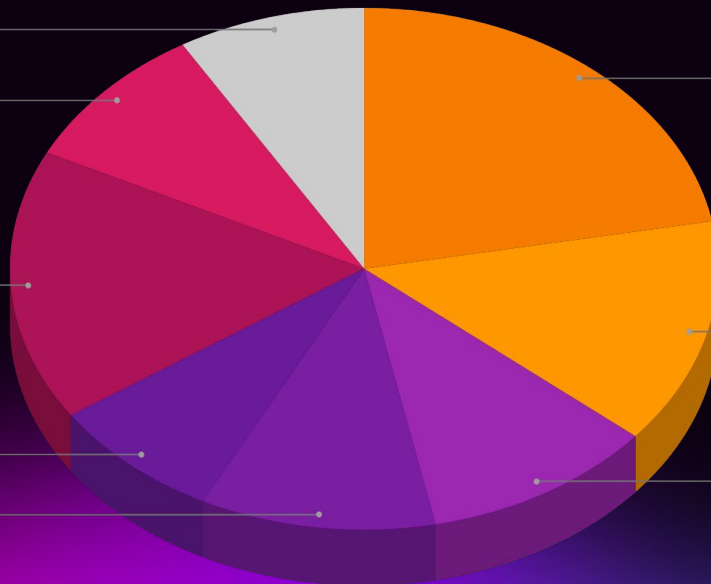
22.1%

**Stored Cross-Site Scripting**

14.0%

**Vertical Privilege Escalation**

10.6%



# Critical bugs



# Exceptional People

*"We pulled some tricks out of our hats to escalate a CSS injection to LFI and SSRF"*

Unleashing the power of CSS injection: The access key to an internal API

<https://sanderwind.medium.com/unleashing-the-power-of-css-injection-the-access-key-to-an-internal-api-789b166d0527> 



daniel\_visma [ company ]

11/5/2021, 1:56:29 PM

Hi!

Thanks a lot [redacted] This is an awesome finding and it is also a very well written report. Taking advantage of the internal API being accessible and in combination with the elasticsearch service we can get pretty much all customer data.

We appreciate your finding and we decided to raise the severity from `Critical` to `Exceptional`.

Regards & Happy Hunting!  
Visma Application Security Team



ioana\_visma [ company ]

11/5/2021, 1:59:00 PM

[redacted] I have the honor of rewarding you for this amazing report. Thanks a lot, we really enjoyed it! And because this is the First Exceptional that we got, it qualifies for a bonus that I will right away give it to you: additional 1337 € will come.

Congrats, once again!

Love, Mother!



# 9,337 €

## TOTAL PAYOUT



# Is it worth it?

Our all time stats



**5500+**

Submissions



**€ 11,390**

Global Average/product



**€100 - €7500**

Bounties



**98%**

Validity



**€1,750**

Global median



**€1M+**

Total bounties

# Making it successful



## Speed

- ✓ Triage
- ✓ Pay
- ✓ Resolve



## Maintain hacker's engagement

- ✓ Be fair & explain decisions
- ✓ Be consistent
- ✓ Special events
- ✓ Support

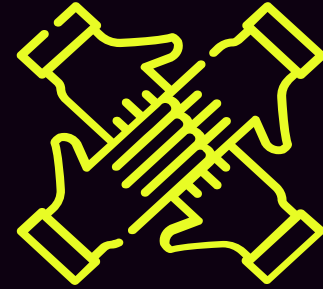


## Transparency

- ✓ With internal teams
- ✓ With hackers
- ✓ With customers

# Key takeaways

- » Bug bounty culture isn't about blame
- » Not all hackers are malicious
- » Team work
- » Hacker mindset
- » Increased confidence
- » Better stress management
- » Knowledge sharing



# Useful links

[What is ethical hacking \(Visma\)](#)

[More about Visma's bug bounty programs \(Visma\)](#)

[An introduction to crowdsourced security for businesses \(Intigrity\)](#)

[The 3 key stages to setting up and managing a bug bounty program \(Intigrity\)](#)

[The Ethical Hacker Insights Report 2022 \(Intigrity\)](#)

Link to this presentation: <http://visma.se/blogg>

# Thank you!



@HackersMother



[linkedin.com/in/ioana-piroska](https://www.linkedin.com/in/ioana-piroska)



[ioana.piroska@visma.com](mailto:ioana.piroska@visma.com)



Visma  
Security Program



# Questions?

The floor is open for discussions

