OWASP
Open Web Application
Security Project

YogOsha
Bug Bounty Platform

Bug Bounty

Marché • Usages • Cas pratiques

OWASP
Open Web Application
Security Project

Yassir Kazar

Cofondateur & CEO Yogosha

- Serial entrepreneur
- chroniqueur cyber-sécurité ZDnet/CafeineTV
- Lead Auditor
- Enseignant Infosec offensive

OWASP

Open Web Application Security Project

Trend Google

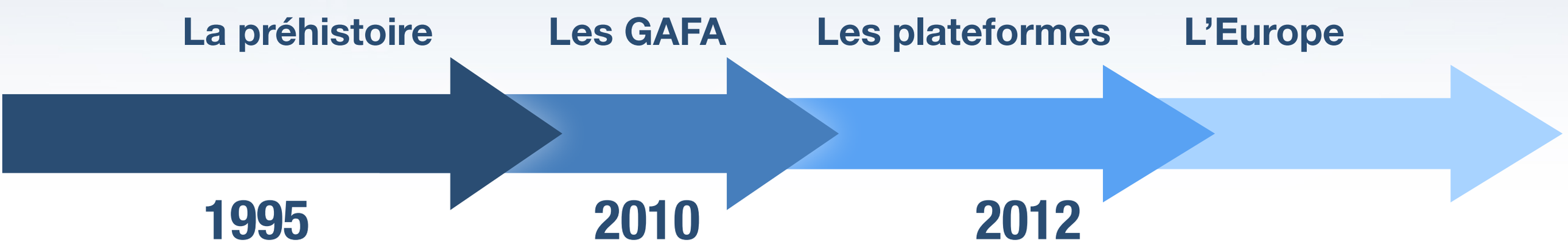
OWASP
Open Web Application
Security Project

ACTE I

Il était une fois...

OWASP
Open Web Application
Security Project

L'Histoire du Bug Bounty



OWASP

Open Web Application Security Project

NETSCAPE

1994

iDEFENSE

VeriSign

2002

mozilla FOUNDATION

2004

ZERO DAY INITIATIVE

TippingPoint

2005

PWN2OWN

CAN SEC WEST

2007

1995

2009

La préhistoire

OWASP

Open Web Application
Security Project

Google

2010

facebook

2011

2010

2011

Le temps des GAFA

OWASP

Open Web Application Security Project

bugcrowd

2012 hackerone

Synack

2013 CrowdCurity

PayPal YAHOO! Microsoft airbnb at&t HUAWEI Adobe NOKIA UNITED AIRLINES

Dropbox TESLA NETFLIX UBER

TELE2 IBM SAP LinkedIn amazon ebay foursquare BlackBerry Deutsche Telekom WESTERN UNION

2012 2014

L'arrivée des plateformes

OWASP

Open Web Application Security Project

2015

YogOsha

2016

bugbounty

BOUNTY FACTORY.io

YES WE H4CK JOBS

2014

2015

2016

Europe & beyond

OWASP

Open Web Application
Security Project

Meanwhile in the USA...

OWASP

Open Web Application
Security Project

ACTE II

La main invisible du marché

OWASP
Open Web Application Security Project

source : BugCrowd

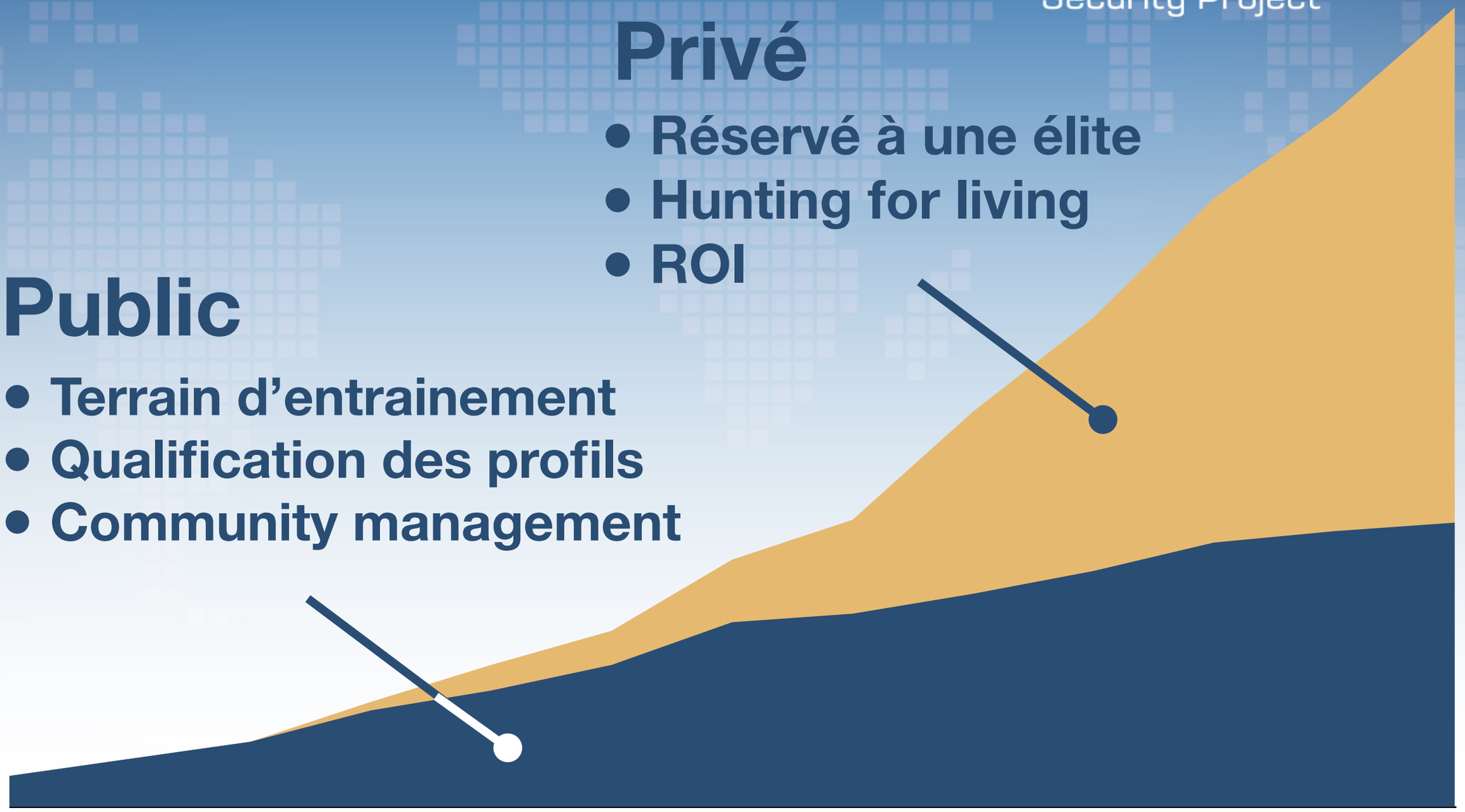
OWASP
Open Web Application Security Project

Privé

- Réservé à une élite
- Hunting for living
- ROI

Public

- Terrain d'entrainement
- Qualification des profils
- Community management

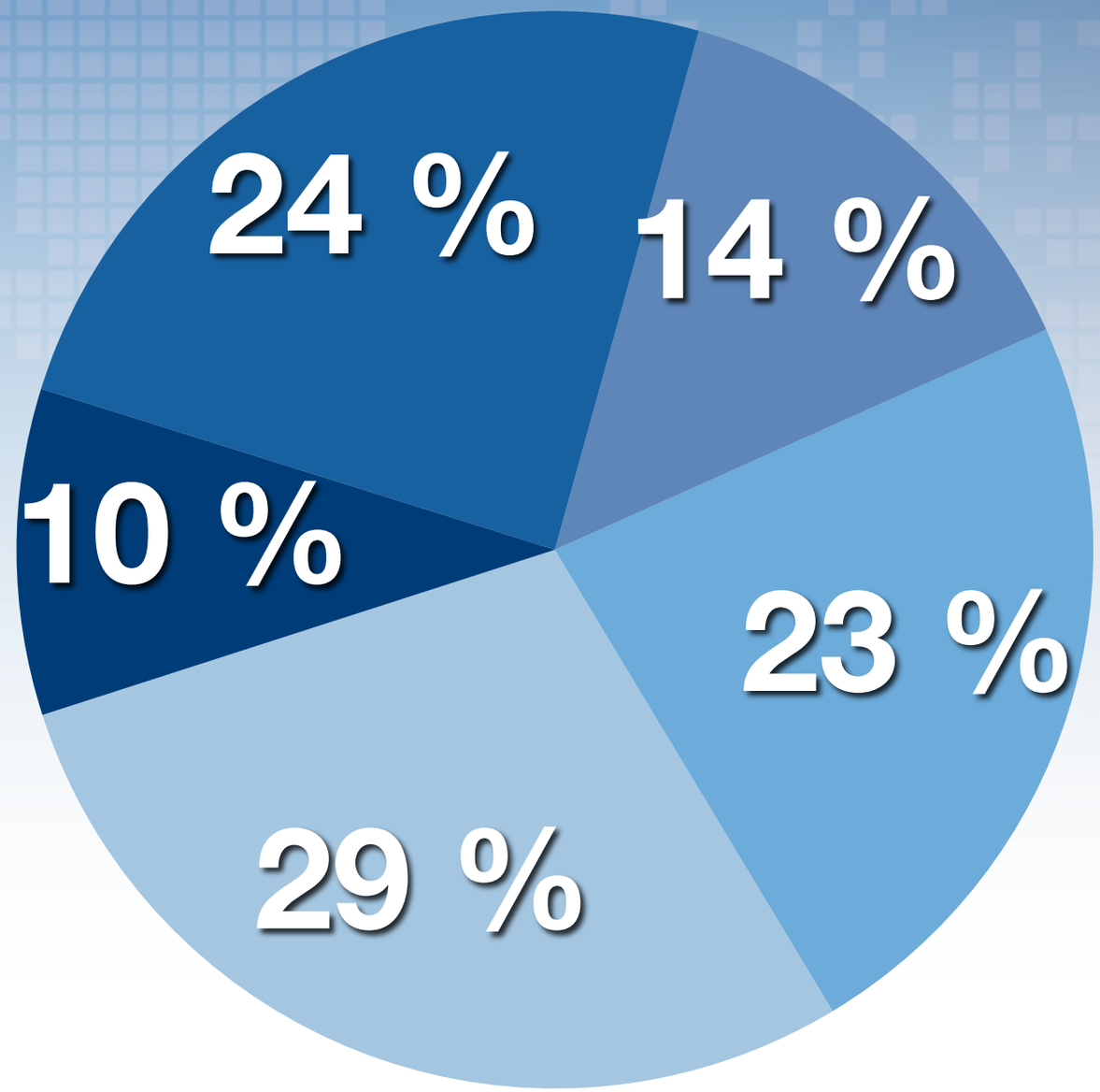


source : BugCrowd

Qui pratique ?

OWASP
Open Web Application Security Project

- +5000
- 500-5000
- 200-499
- 50-199
- 1 à 49

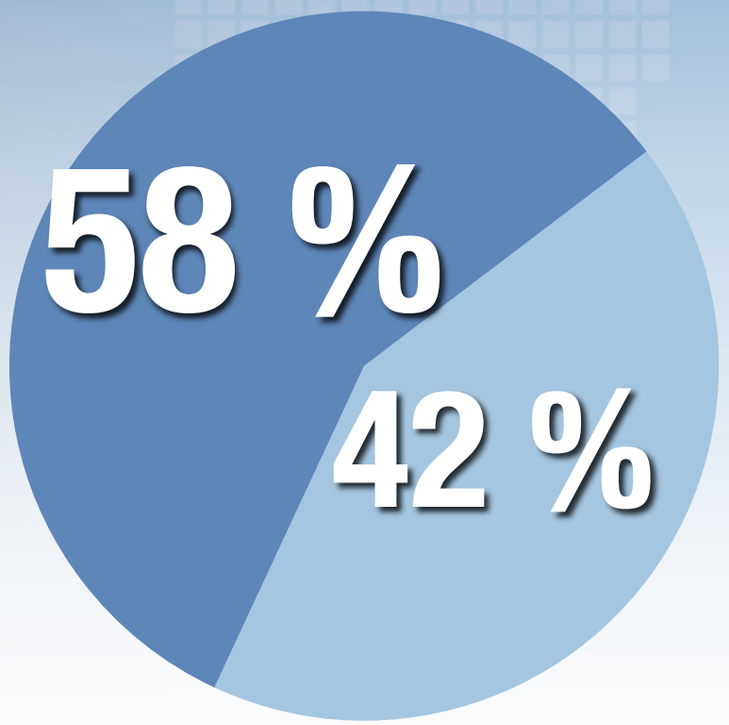


Qui pratique ?

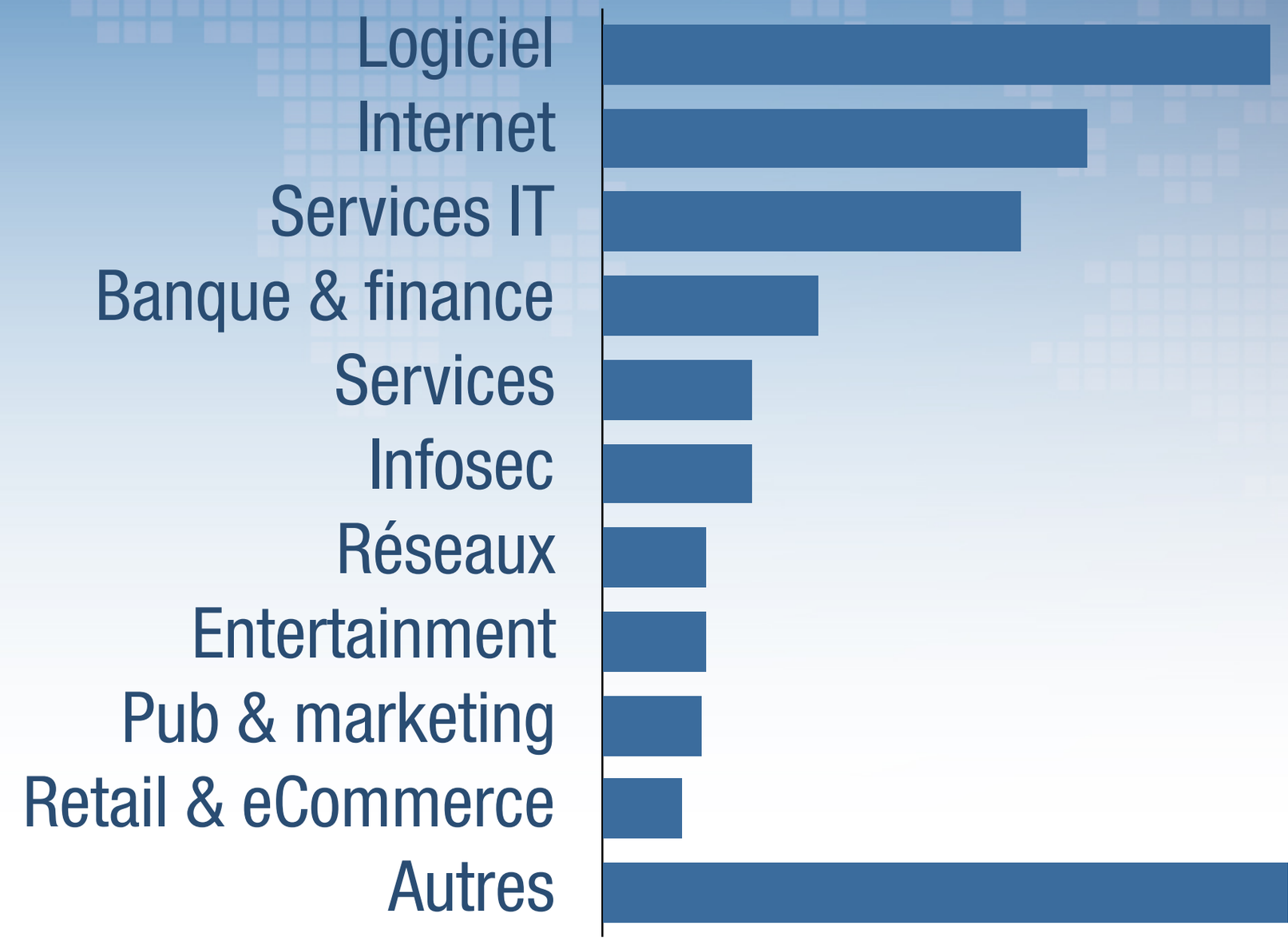
OWASP
Open Web Application Security Project

Qui pratique ?

OWASP
Open Web Application Security Project

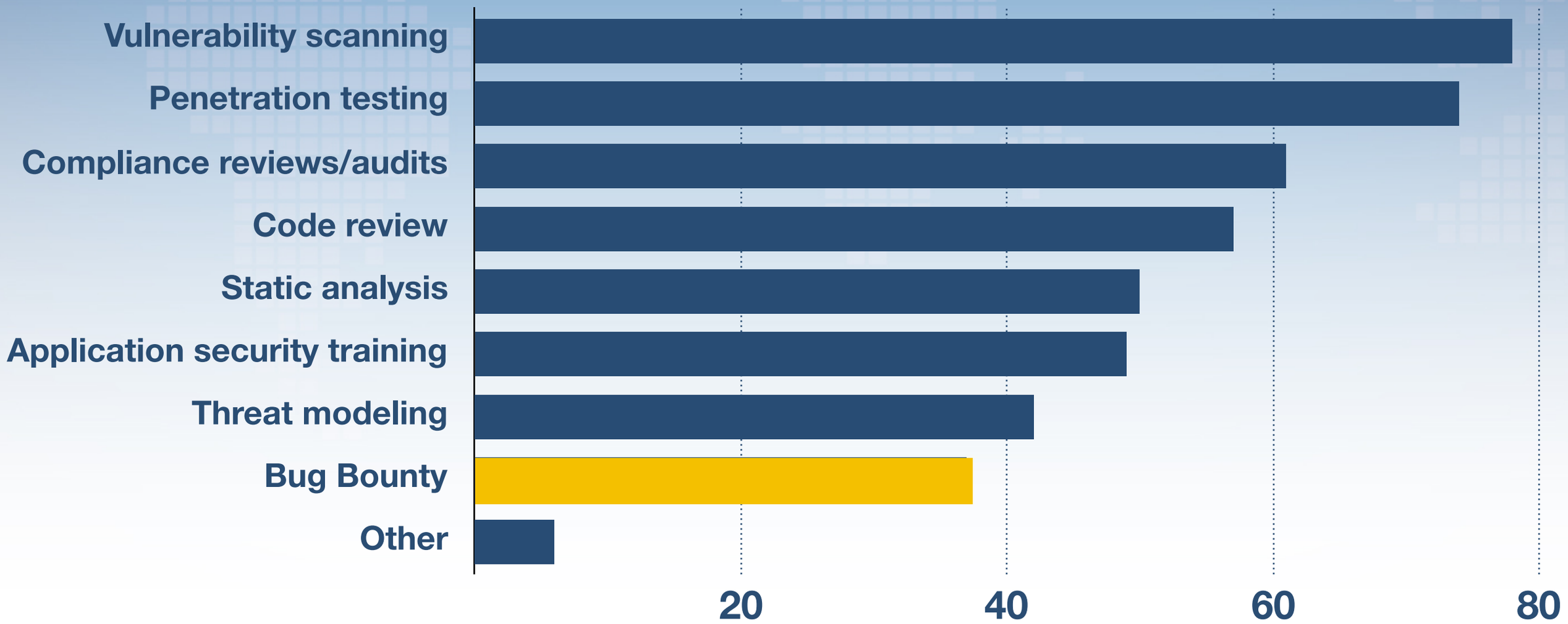


- tech
- non-tech



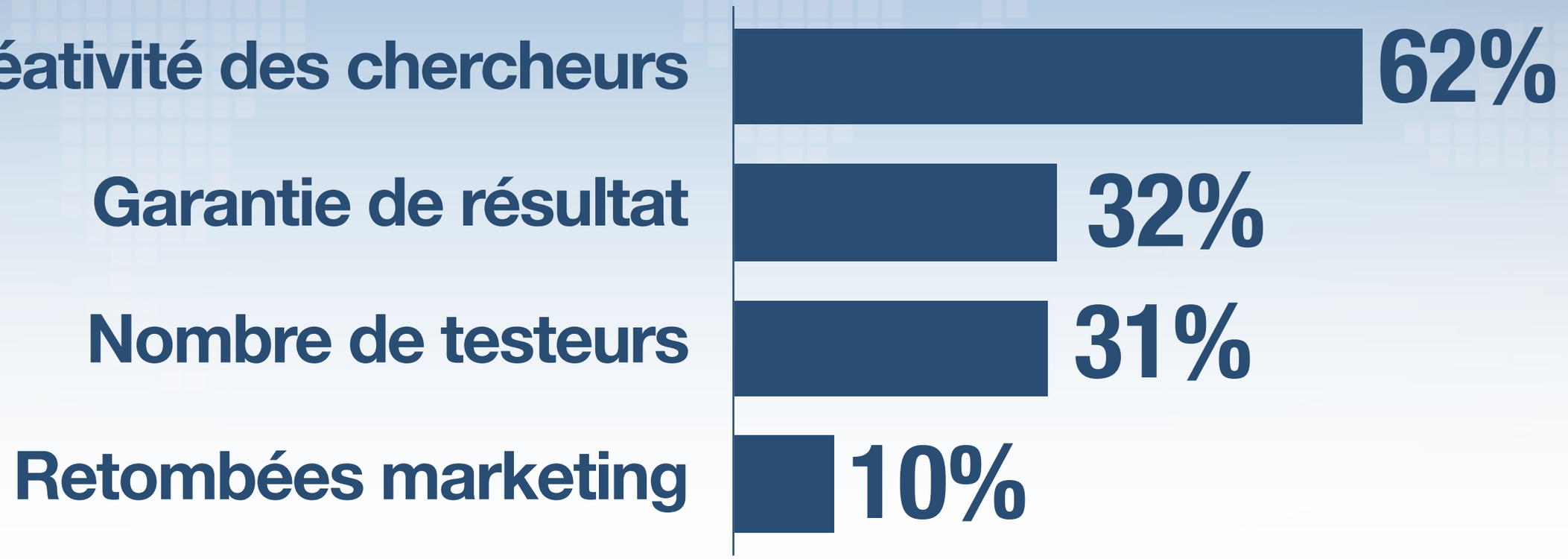
Le Bug Bounty
et les pratiques infosec

OWASP
Open Web Application Security Project



‘Pourquoi choisir un Bug Bounty ?’

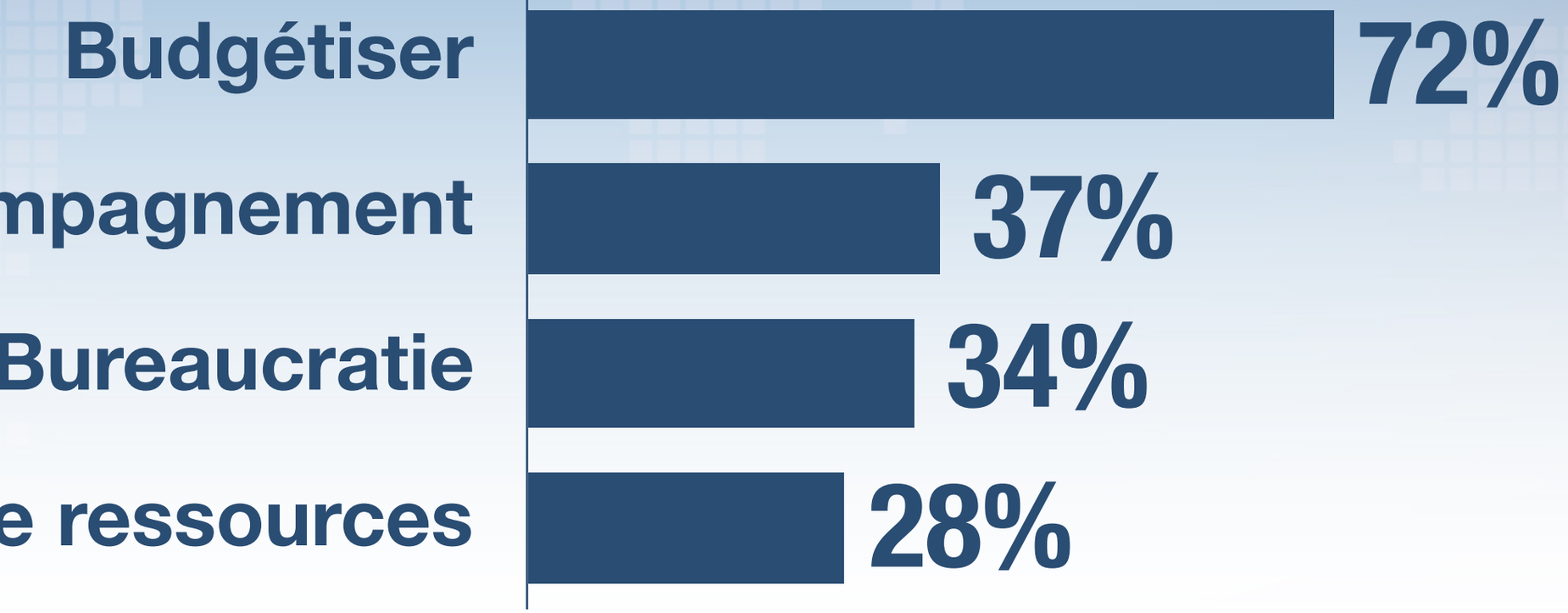
OWASP
Open Web Application Security Project



Sondage fait auprès de 185 experts infosec en charge d’un Bug Bounty dans leur entreprise, source BugCrowd

Les freins au Bug Bounty

OWASP
Open Web Application Security Project



Sondage fait auprès de 315 chasseurs de bug en poste en entreprise, source BugCrowd

OWASP
Open Web Application
Security Project

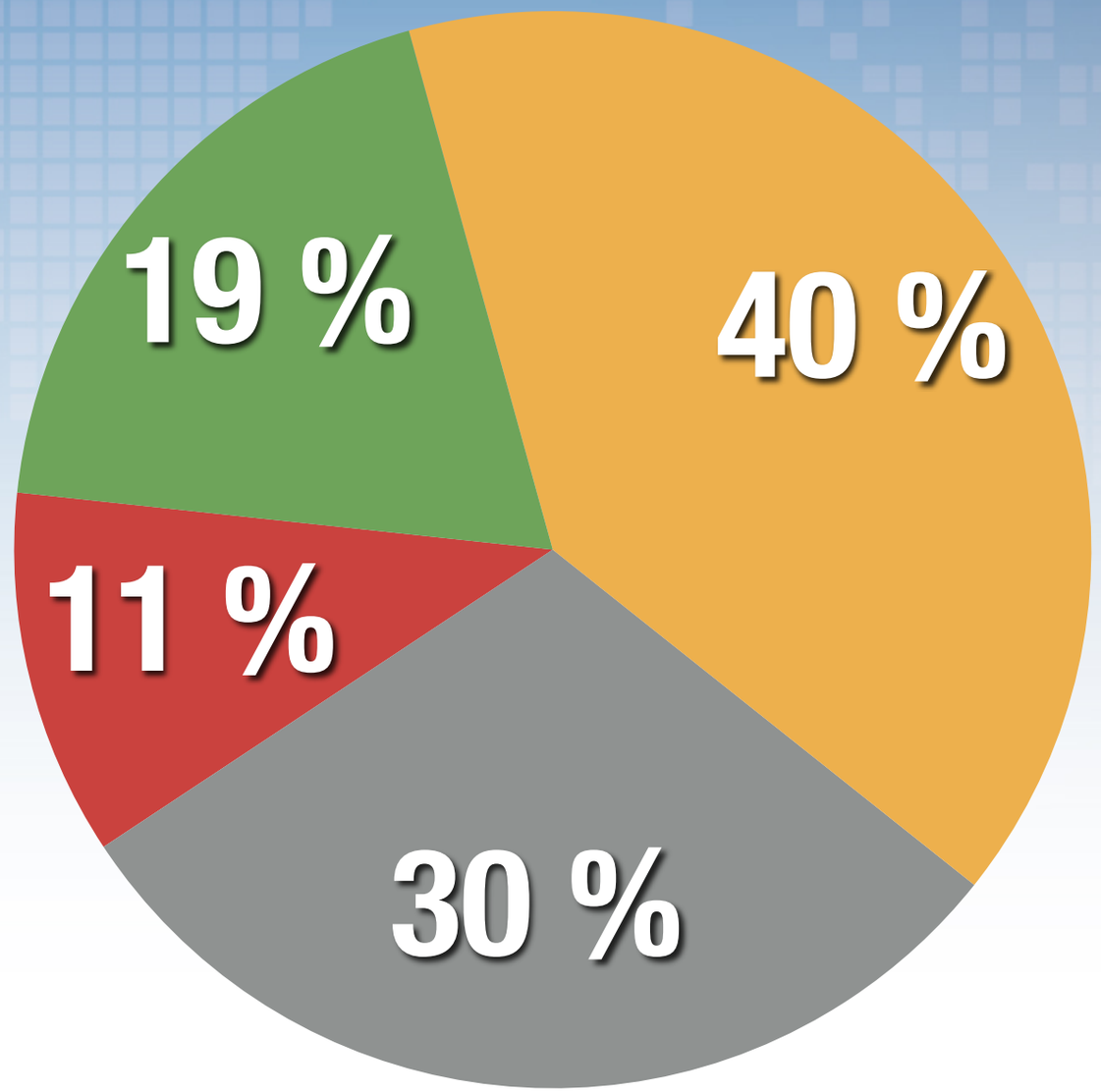
ACTE II

Des chiffres et des Vulns

Trier les rapports entrants

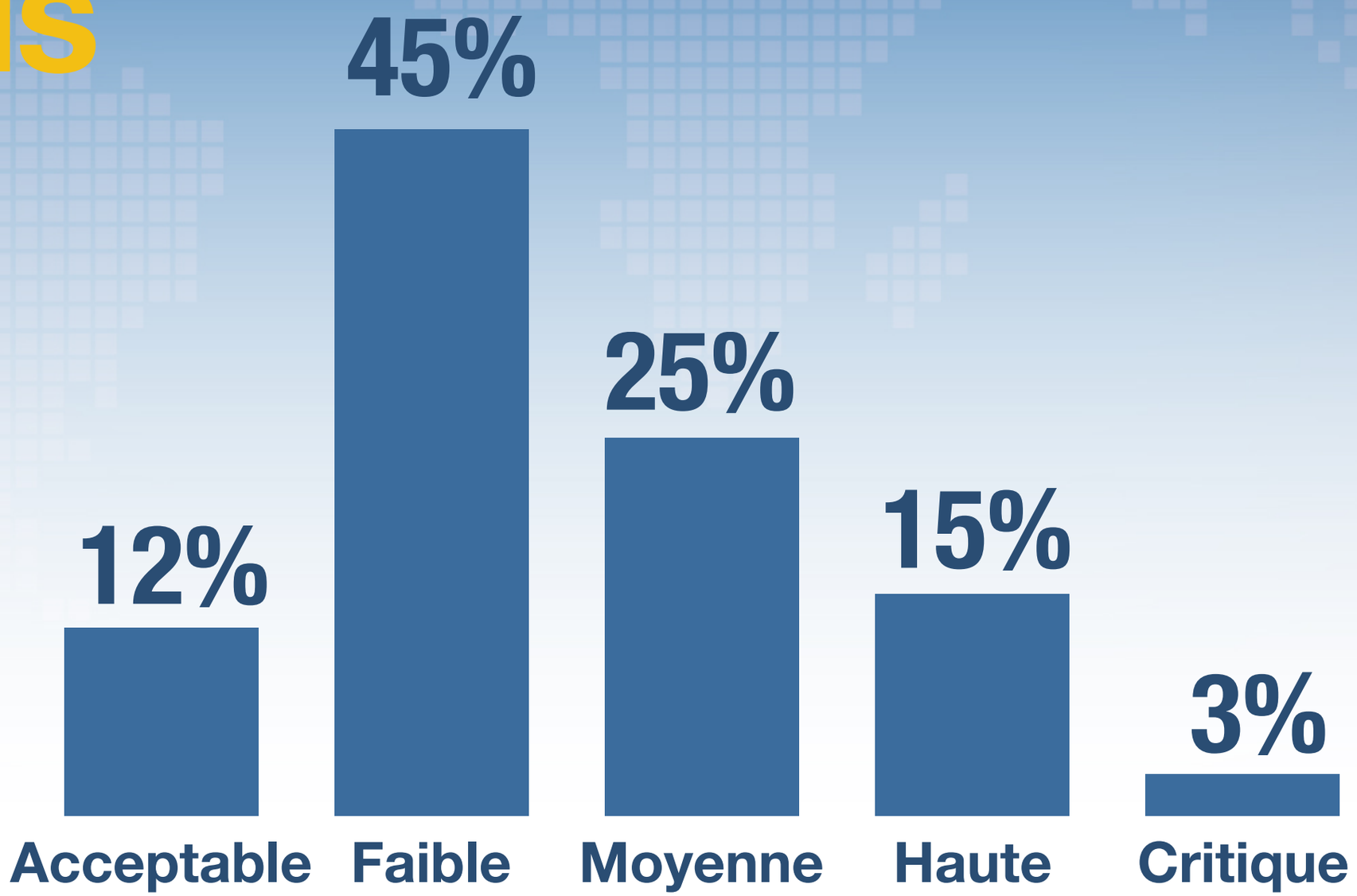
OWASP
Open Web Application Security Project

- Valides
- Duplicatas
- Invalides
- Hors périmètre



Echantillon de 29537 rapports, source BugCrowd

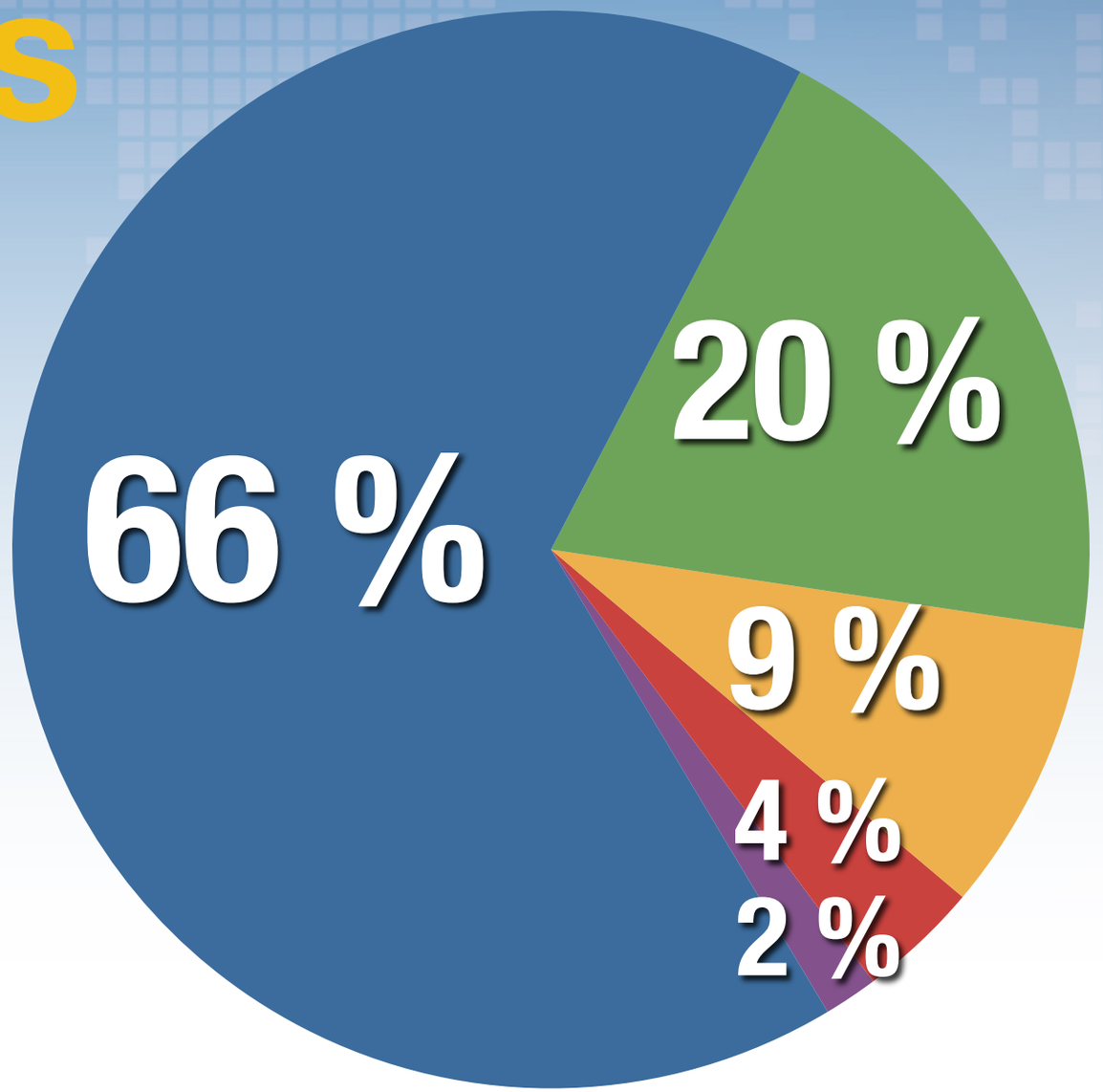
Criticité des rapports reçus



Echantillon de 29537 rapports, source BugCrowd

Typologie des failles découvertes

OWASP
Open Web Application Security Project

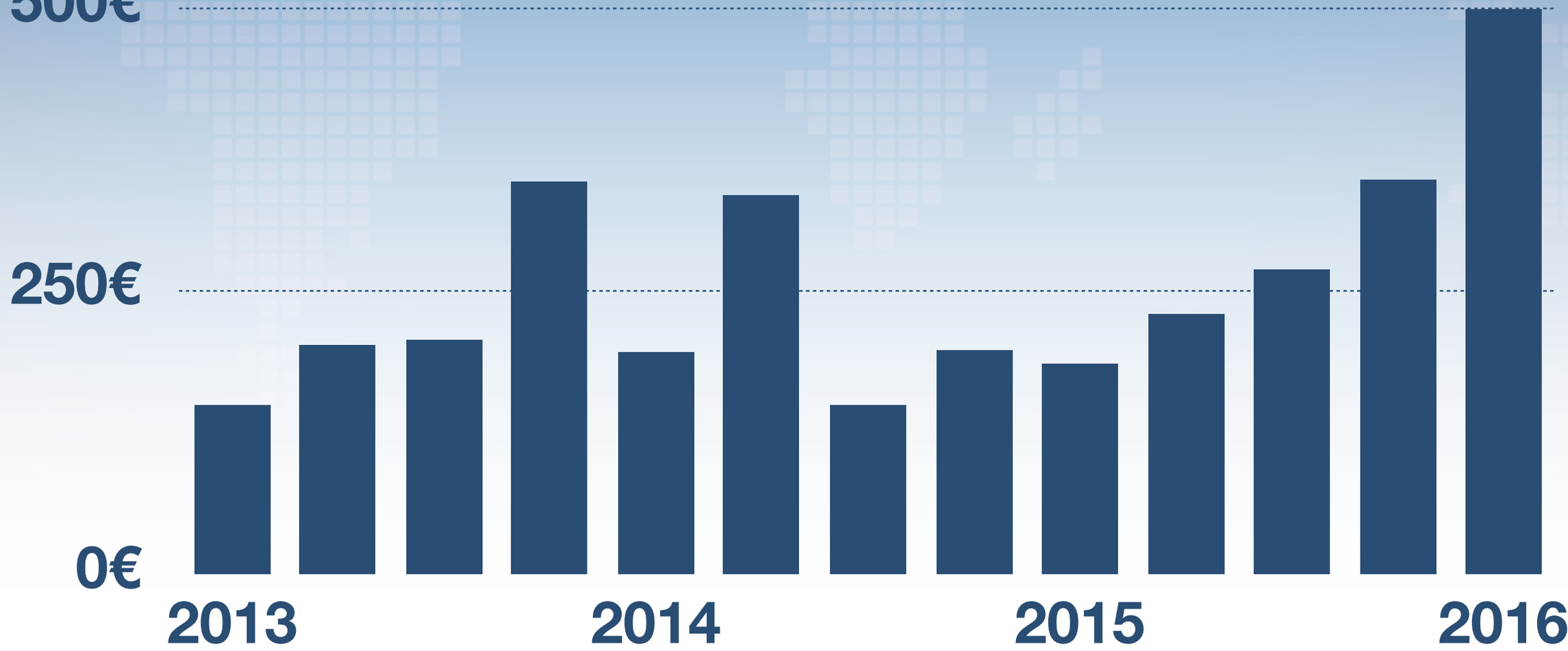


- XSS
- CSRF
- Mobile
- SQLI
- Clickjack

Echantillon de 29537 rapports excluant la catégorie «autres failles», source BugCrowd

Coût moyen par bug

OWASP
Open Web Application Security Project



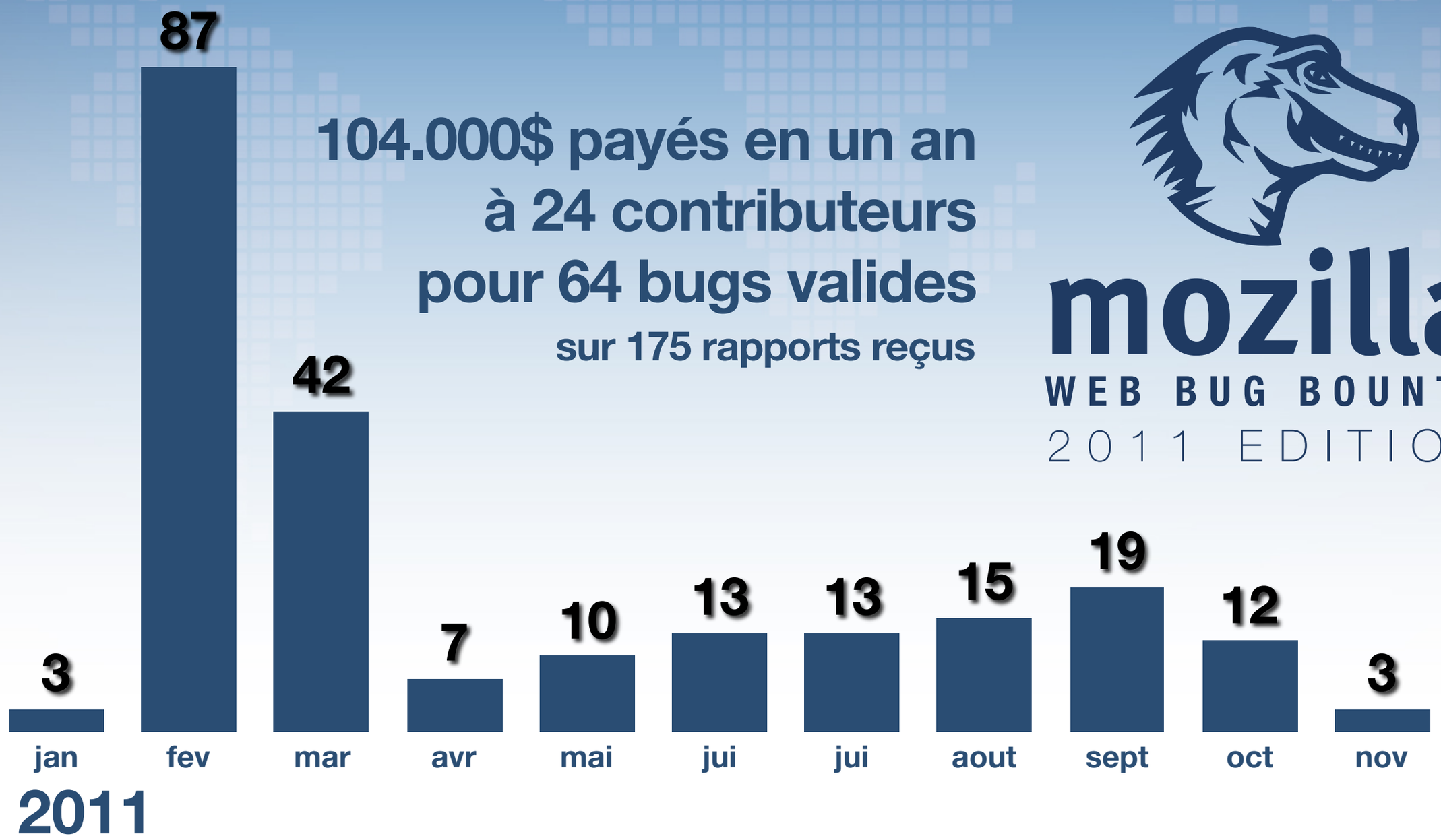
Echantillon de 29537 rapports, source BugCrowd

Case study

OWASP
Open Web Application Security Project

104.000$ payés en un an
à 24 contributeurs
pour 64 bugs valides
sur 175 rapports reçus

mozilla
WEB BUG BOUNTY
2011 EDITION



Case study

OWASP
Open Web Application Security Project

160

GitHub
BUG BOUNTY EDITION 2014

106,667

- 1920 rapports reçus
- 73 vulnérabilité trouvées
  dont 57 d'une criticité moyenne ou haute.
- Des bugs dont le prix va de 200$ à 10.000$
  33 chercheurs ont gagné à eux seuls plus de 50k$

53,333

Case study

OWASP
Open Web Application
Security Project

facebook®

BUG BOUNTY 2014

- 123 pays participants
- plus de 17.000 bugs soumis
- 61 bugs critiques reçus
- 1,3M$ payés à 321 chercheurs

Case study

OWASP
Open Web Application
Security Project

Google

BUG BOUNTY 2015

- 2,5M$ de budget
- +6M$ en six ans
- 200 hackers récompensés
- 500 failles identifiées

OWASP

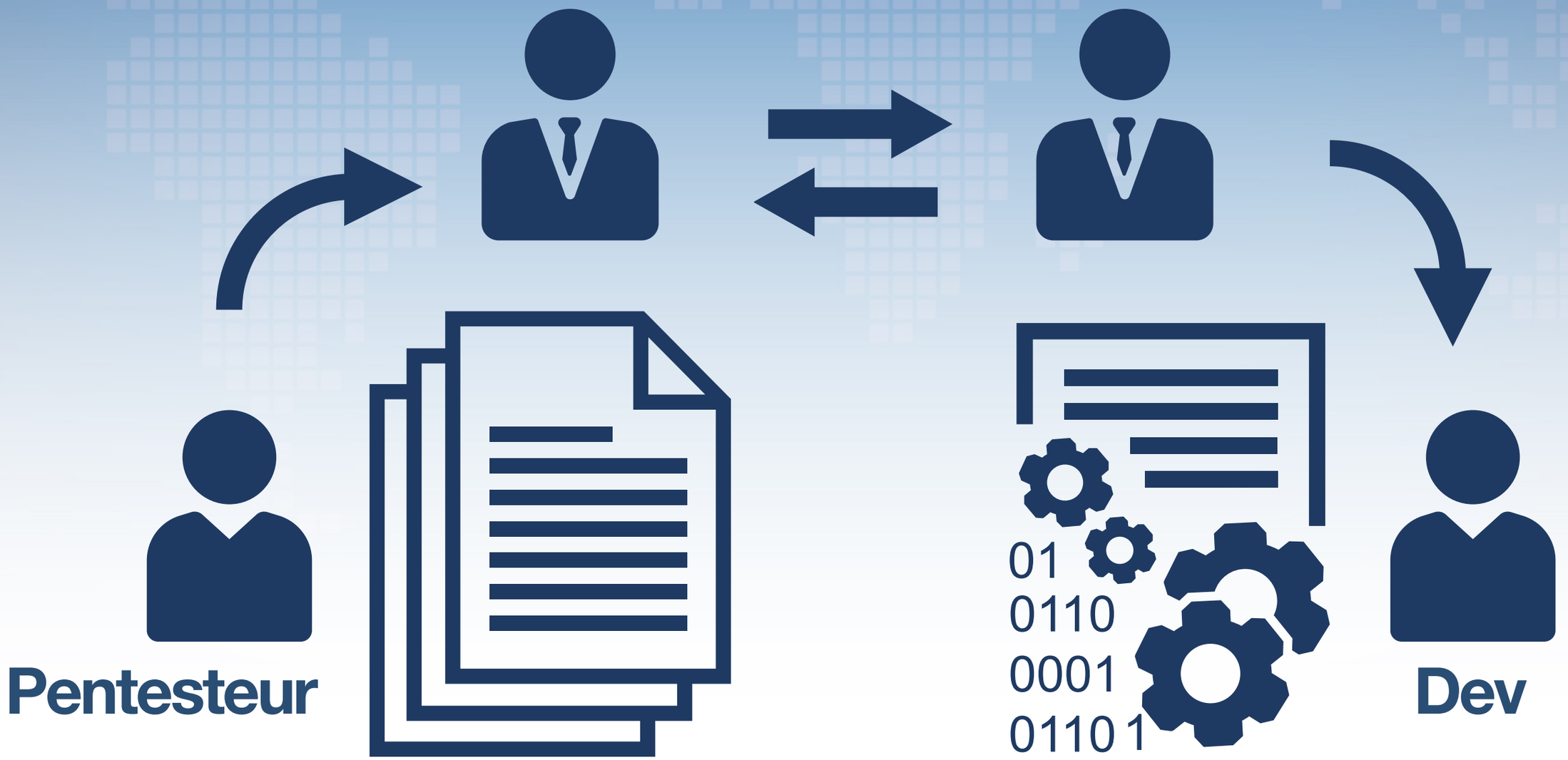
Open Web Application
Security Project

ACTE IV

Travailler autrement

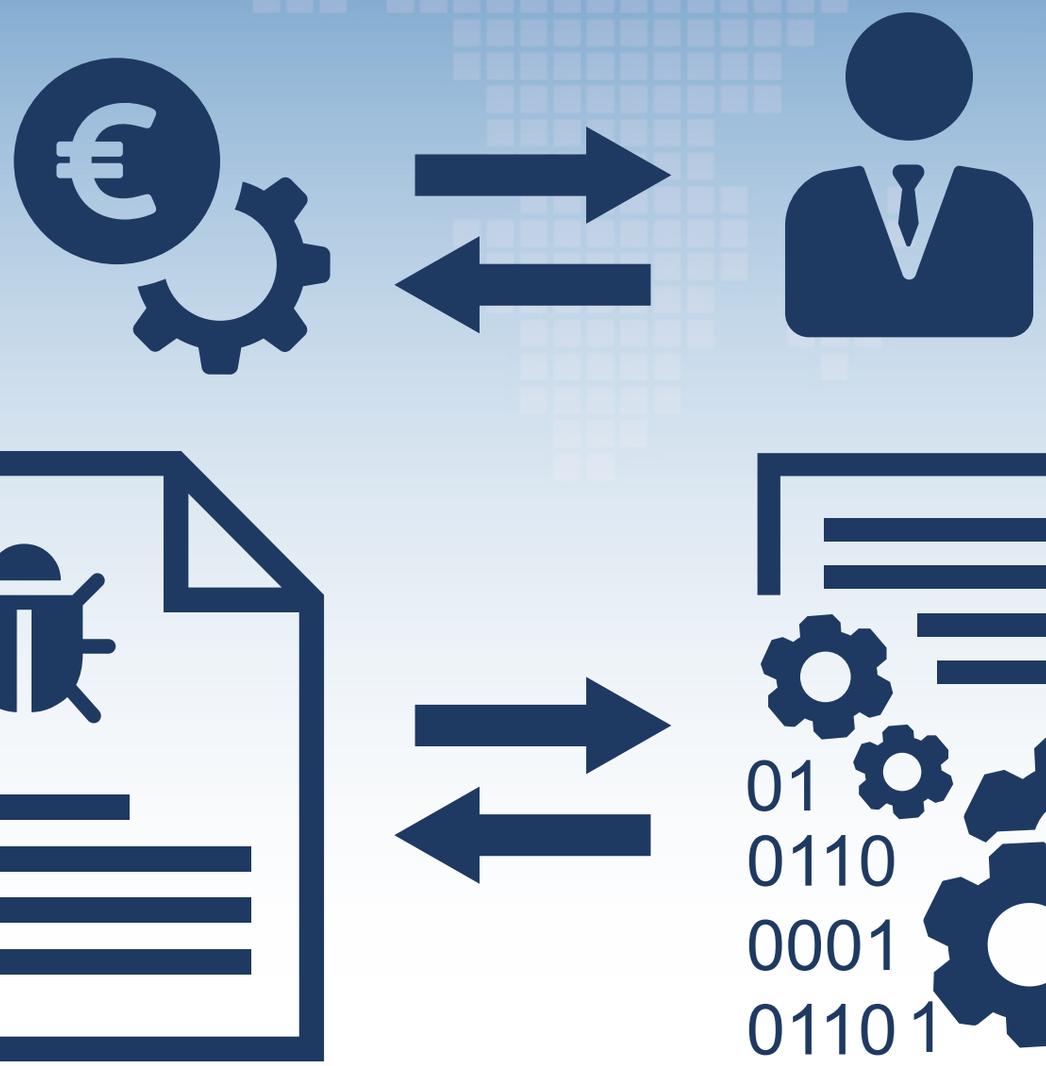
Pentesting

OWASP
Open Web Application
Security Project



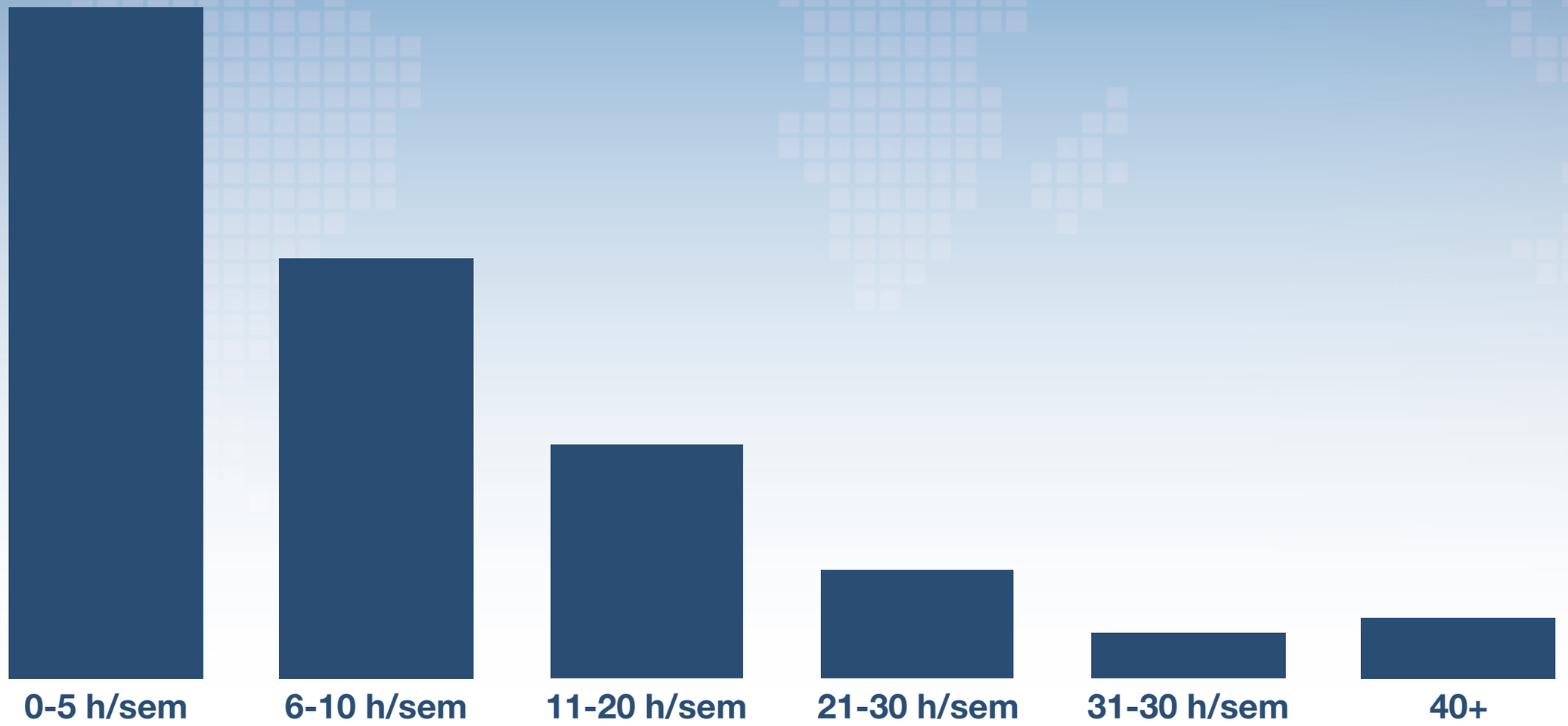
Pentesting

OWASP
Open Web Application
Security Project



Temps de travail

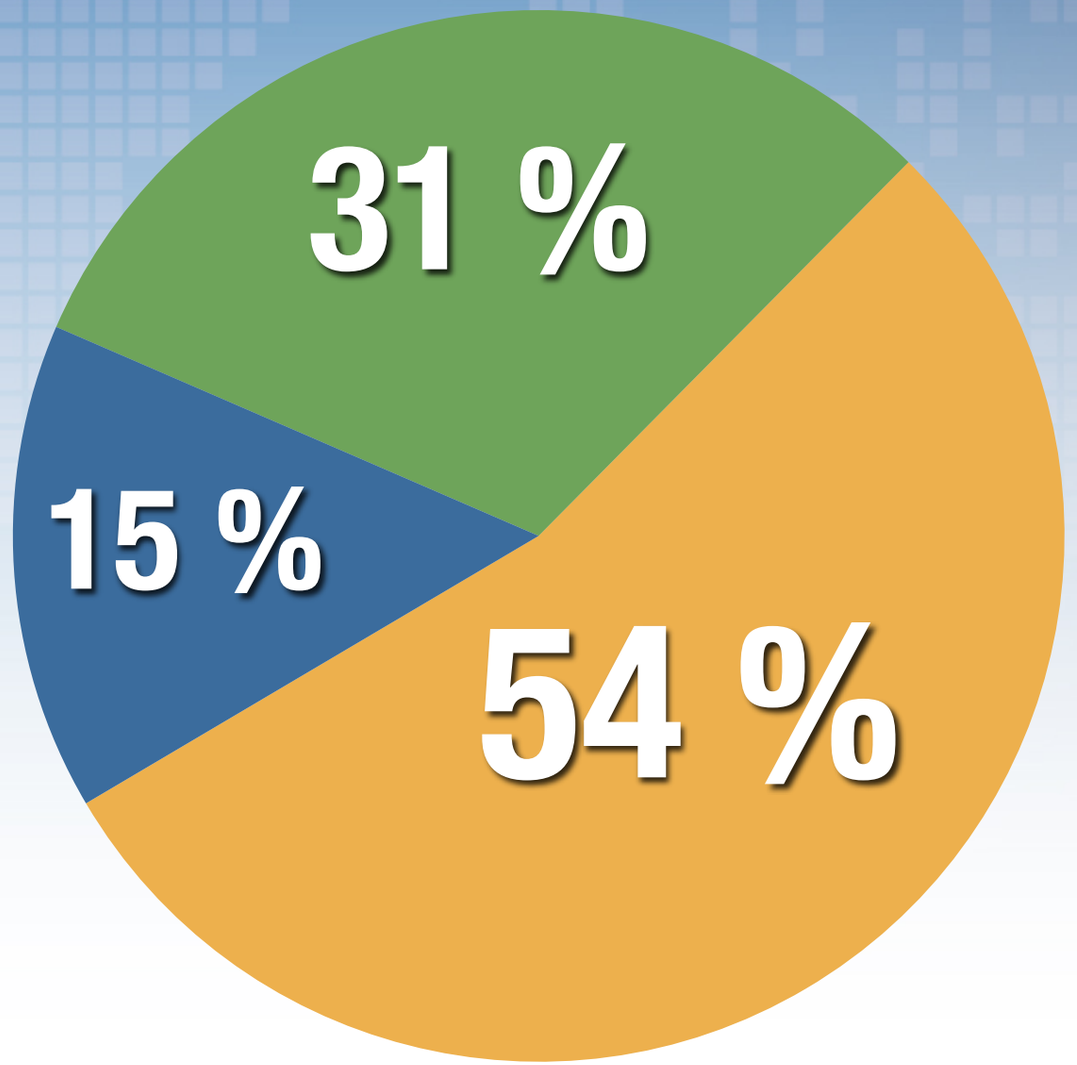
OWASP
Open Web Application Security Project



Sondage fait auprès de 500 chasseurs de bug, source BugCrowd

Un métier à plein temps ?

OWASP
Open Web Application Security Project



- Plein temps
- Objectif plein temps
- Complément

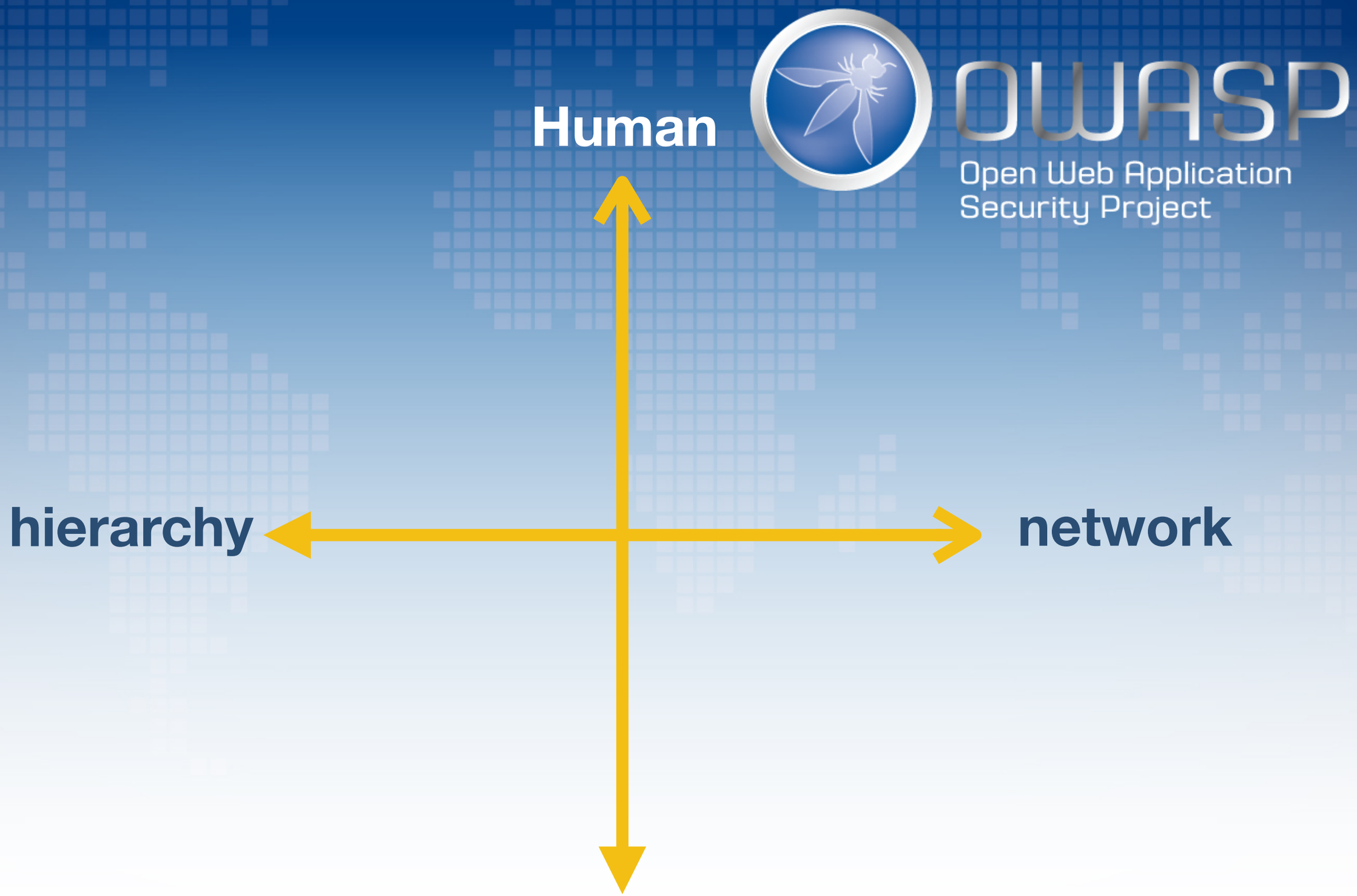
Sondage fait auprès de 500 chasseurs de bug, source BugCrowd

Répartition des revenus

OWASP
Open Web Application Security Project

Répartition des revenus

OWASP
Open Web Application Security Project



OWASP

Open Web Application Security Project

OWASP

Open Web Application
Security Project

DevOpsSec

OWASP
Open Web Application
Security Project

EPILOGUE

OWASP & Bug Bounty

OWASP

Open Web Application
Security Project

Merci

y.kazar@yogosha.com