Innovate, Navigate, Elevate:

A Journey into OffSec Entrepreneurship

x33fcon June 2024

Marc Smeets
@MarcOverIP

x33fcon

OUTFLANK

ABOUT YOUR SPEAKER

Marc Smeets - @MarcOverIP

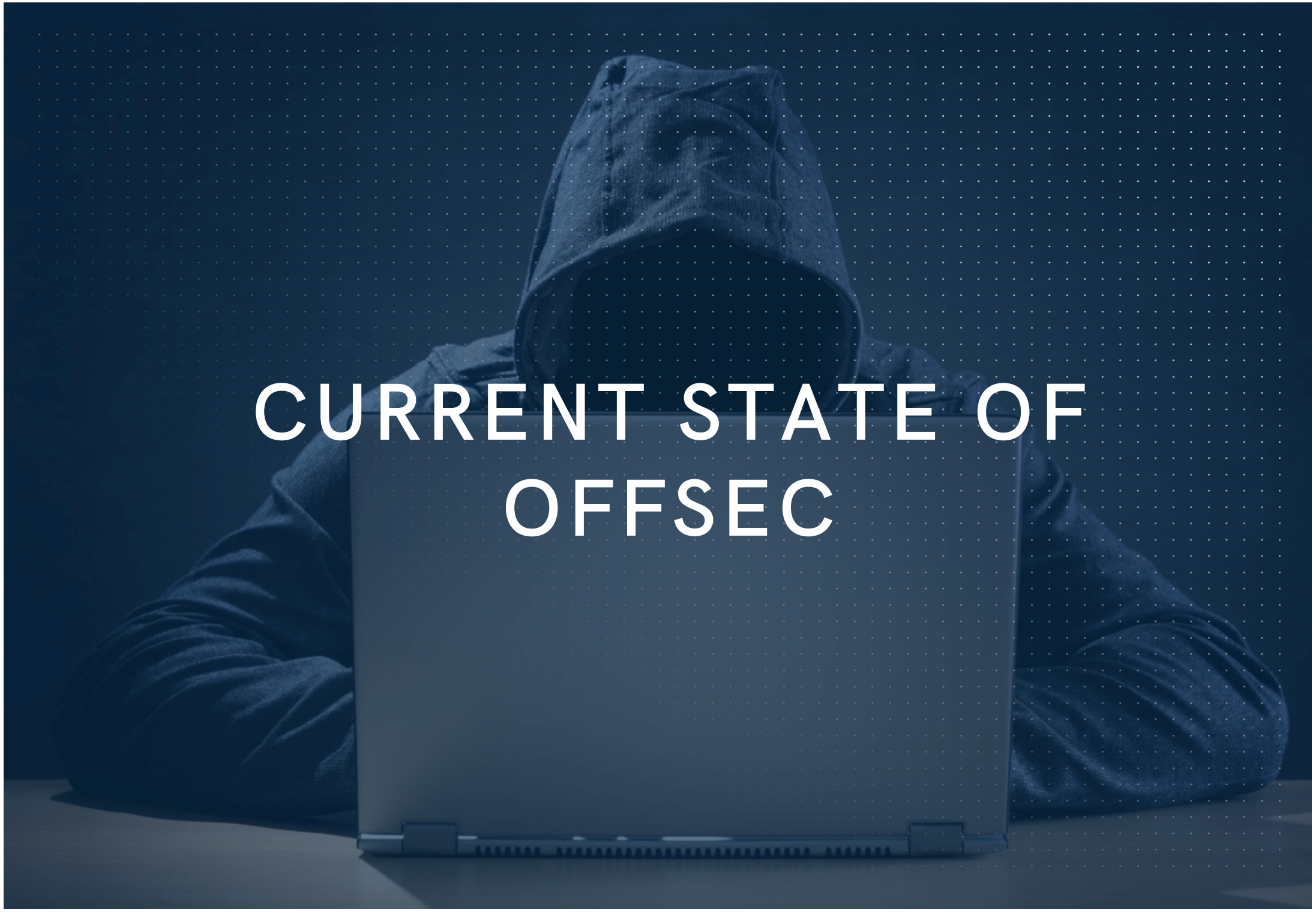
- Infosec class of 1999 (hobby) / 2006 (professionally)
- Background in network engineering, pentesting and red teaming
- Employee (7yr), free lancer (3yr), co-founder (6yr), acquired (2yr+)

Outflank - @OutflankNL

- Specialised in red team tooling and tradecraft
- Private 'Outflank Security Tooling' available via:
  - https://outflank.nl/OST
- Public tools and blogs via:
  - https://outflank.nl/blog
  - https://github.com/OutflankNL


TURN TO CLEAR VISION
QUARTERS ONLY
25¢
TO OPERATE
STEP 1
STEP 2
WOODEN
SHOE
TULIP FARM


IDEA


CURRENT STATE OF
OFFSEC

THE YEAR IS 2024 – RED HAS SERIOUS CHALLENGES

- **No more GitCloneYOLOToDA**
  - EDRs are stronger
  - Red teaming has become a lot more complex
  - Less tools shared publicly

- **Blue is the new sexy**
  - Effective SOC
  - Blue has learned to use quick feedback cycles
  - More budget available


“ Change is the law of life. And those who look only to the past or present are certain to miss the future. ”
– John F. Kennedy

RED NEEDS TO ADAPT TO NEW FACTS

1. RT is hard: invest || GTFO

We've done this before:

- Commercial vulnerability scanning tools, Metasploit Pro, Bug bounties
- Commercial C2 Cobalt Strike

Positive changes happening now:

- Paid full tools:
  BallisKit, Evilginx, Nighthawk, Outflank Security Tooling
- Paid R&D:
  Outflank Security Tooling

2. Red struggles with public sharing

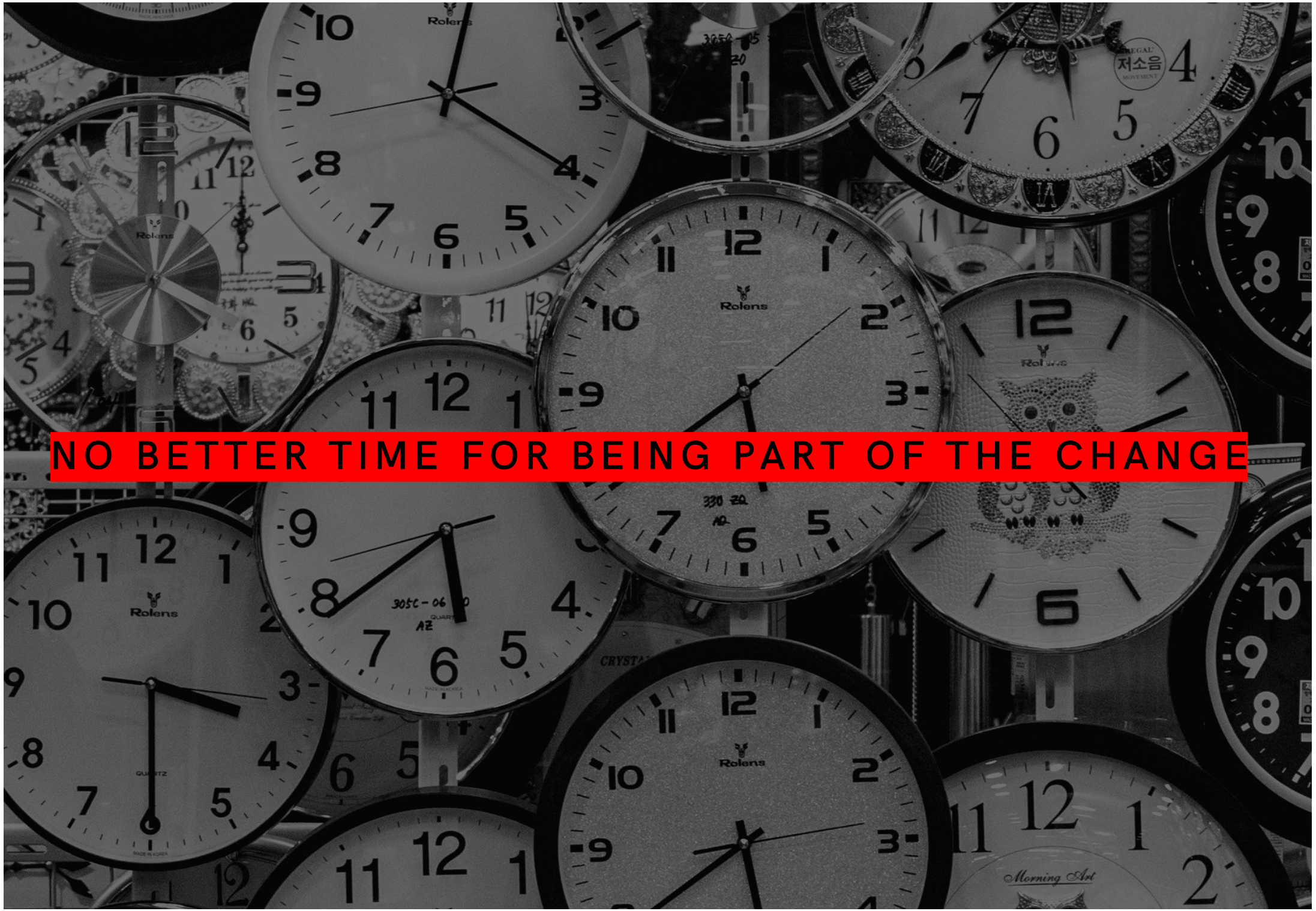
Before this was different:

- OST debate != SAINT or Mimikatz
- Ransomware / APTs make it different

Positive changes happening now:

- Smaller 'trusted' circles
- Blogs come with limited PoCs and/or detailed detection rules

Have you picked your idea yet?

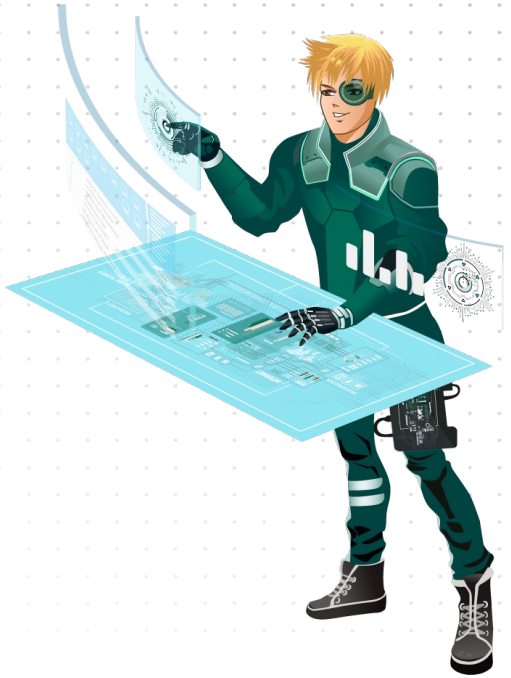

NO BETTER TIME FOR BEING PART OF THE CHANGE


ENTREPRENEURSHIP 101

LEARNING FROM OTHERS

OUTFLANK

red team tooling & tradecraft



PORCHETTA INDUSTRIES

CASE STUDY: OUTFLANK – THE START

2016:

- Aim is start a red teaming consulting firm and have fun
- Market not really ready for red teaming
- Easy choice to license Cobalt Strike
- Quality in *everything*

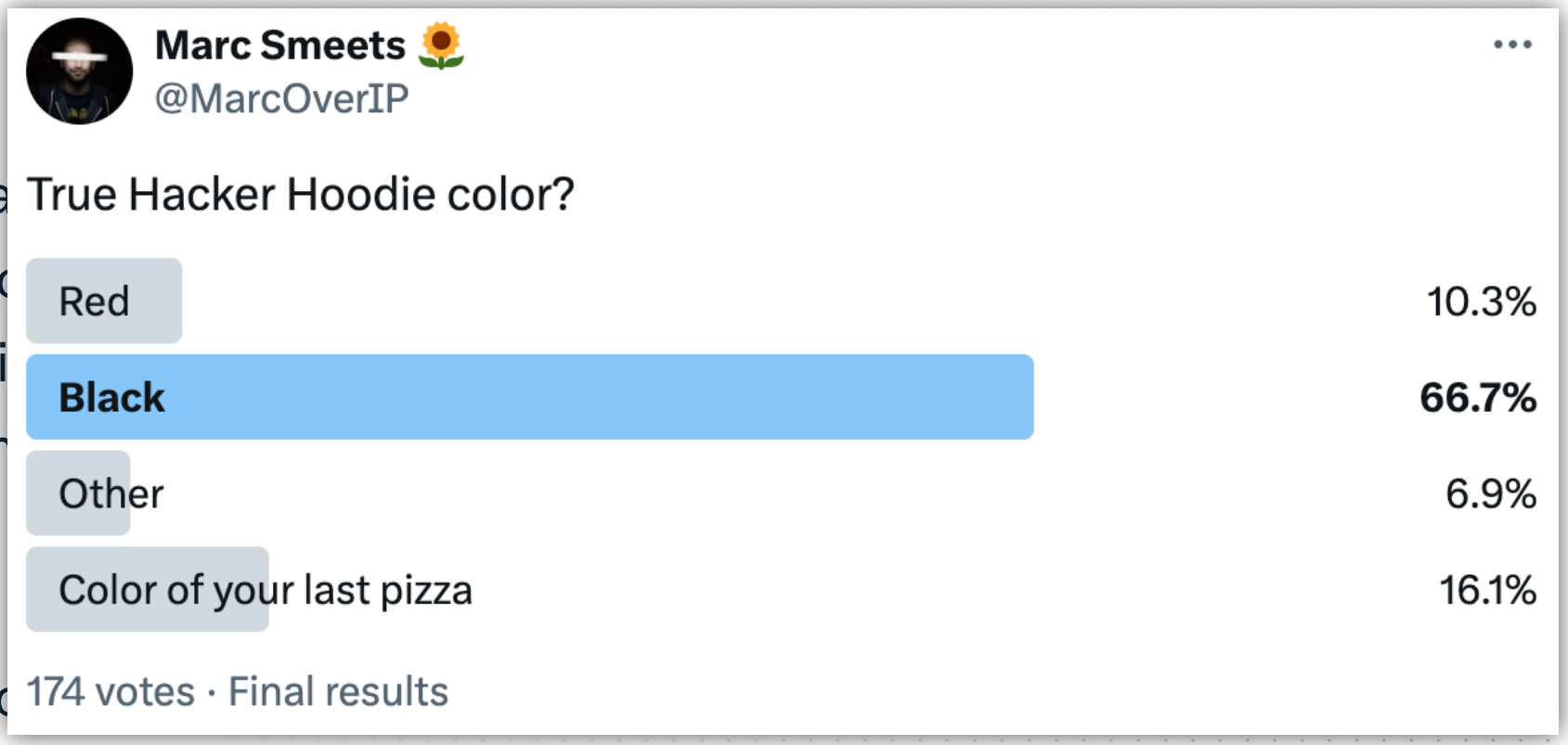
- Goal was to build a name in the industry:
  - We personally were no-names in the industry
  - Spent a lot of time on initial launch (name, org setup, logo, etc.)
  - Red hoodies by accident
  - Blogs, research, presentations

Invoke-ADLabDeployer NetshHelperBeacon

CASE STUDY: OUTFLANK – THE START

2016:

- Aim is sta
- Market nc
- Easy choi
- Quality ir



- Goal was
  - We persc
  - Spent a lot of time on initial launch (name, org setup, logo, etc.)
  - Red hoodies by accident
  - Blogs, research, presentations

Invoke-ADLabDeployer NetshHelperBeacon

CASE STUDY: OUTFLANK – KNOWN RED TEAM

2019

- High performing small red team
- Keep up blogs, tools and conference talks
- Starting developing inhouse arsenal
- More than the technical tricks you do

CASE STUDY: OUTFLANK – SIDE PRODUCT

2020 - Outflank Security Tooling

- Side product to compensate our R&D efforts
- Heavy internal debates
- Fantastic feedback from potential customers
- Strong built-in product security
- Export Controls

CASE STUDY: OUTFLANK - OST PIVOT

2021

- Selling software != selling consultancy
- Pivoting is hard
- To grow you need to let loose

2022+

- Partnering with Fortra
- Learn how scaling up is done
- Innovate as we go (tradecraft, community, external developers)

Have you picked your idea yet?


What is holding you back?
1,2,3...
LET'S GO!

OUTFLANK

Marc Smeets
@MarcOverIP
marc.smeets@fortra.com
www.outflank.nl/marc