RED TEAM TOOLING

Challenges in TIBER and EDR evasion

Stan Hegt

27 November 2024

OUTFLANK

clear advice with a hacker mindset

WHOAMI

- Co-founder of Outflank
- Red team operator turned holiday-approver (aka CEO)
- Speaker at Black Hat, Troopers, DerbyCon, RedTreat
- Today: user and author of various red teaming tools

OUTFLANK

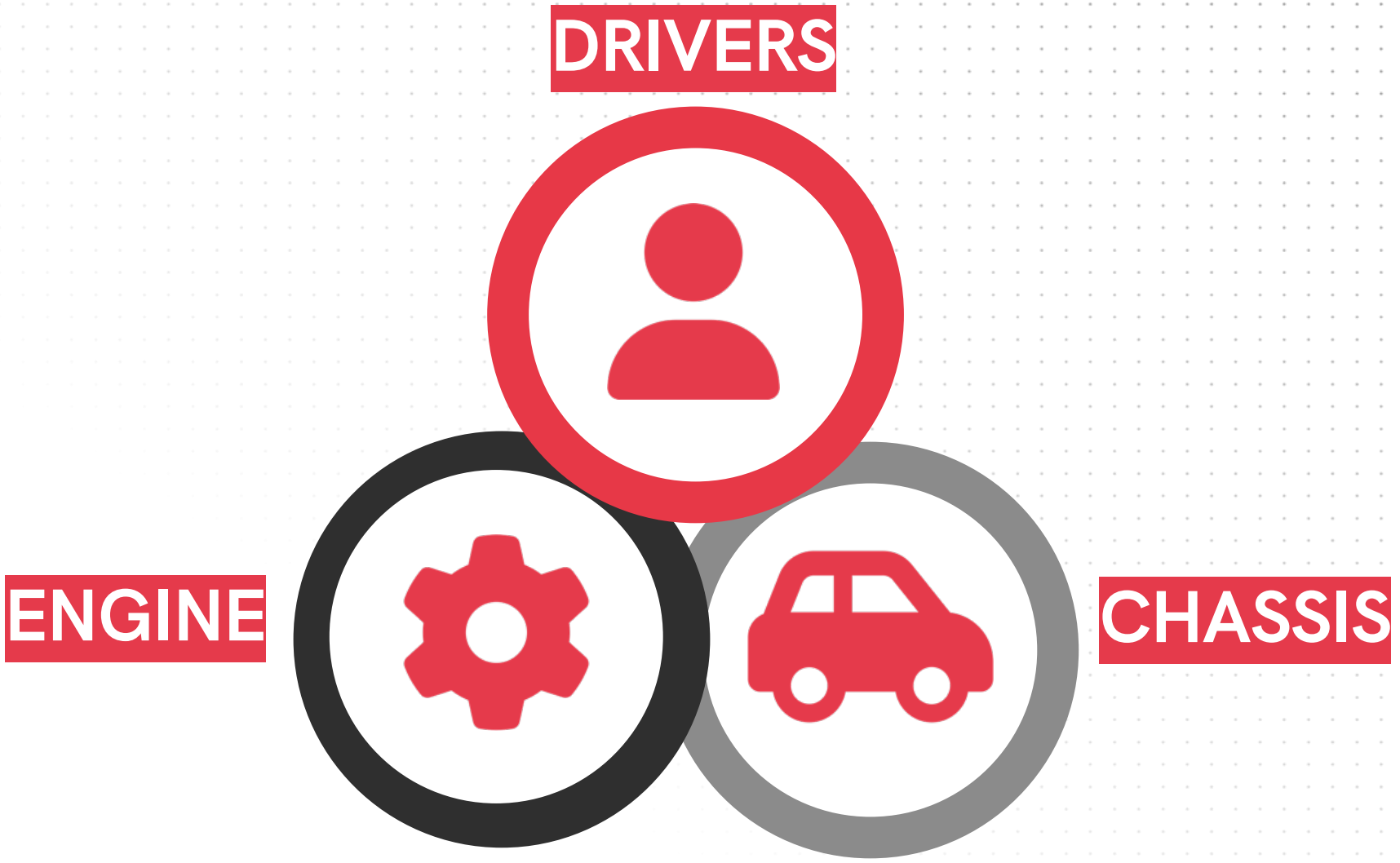
red team tooling & tradecraft

COBALT STRIKE

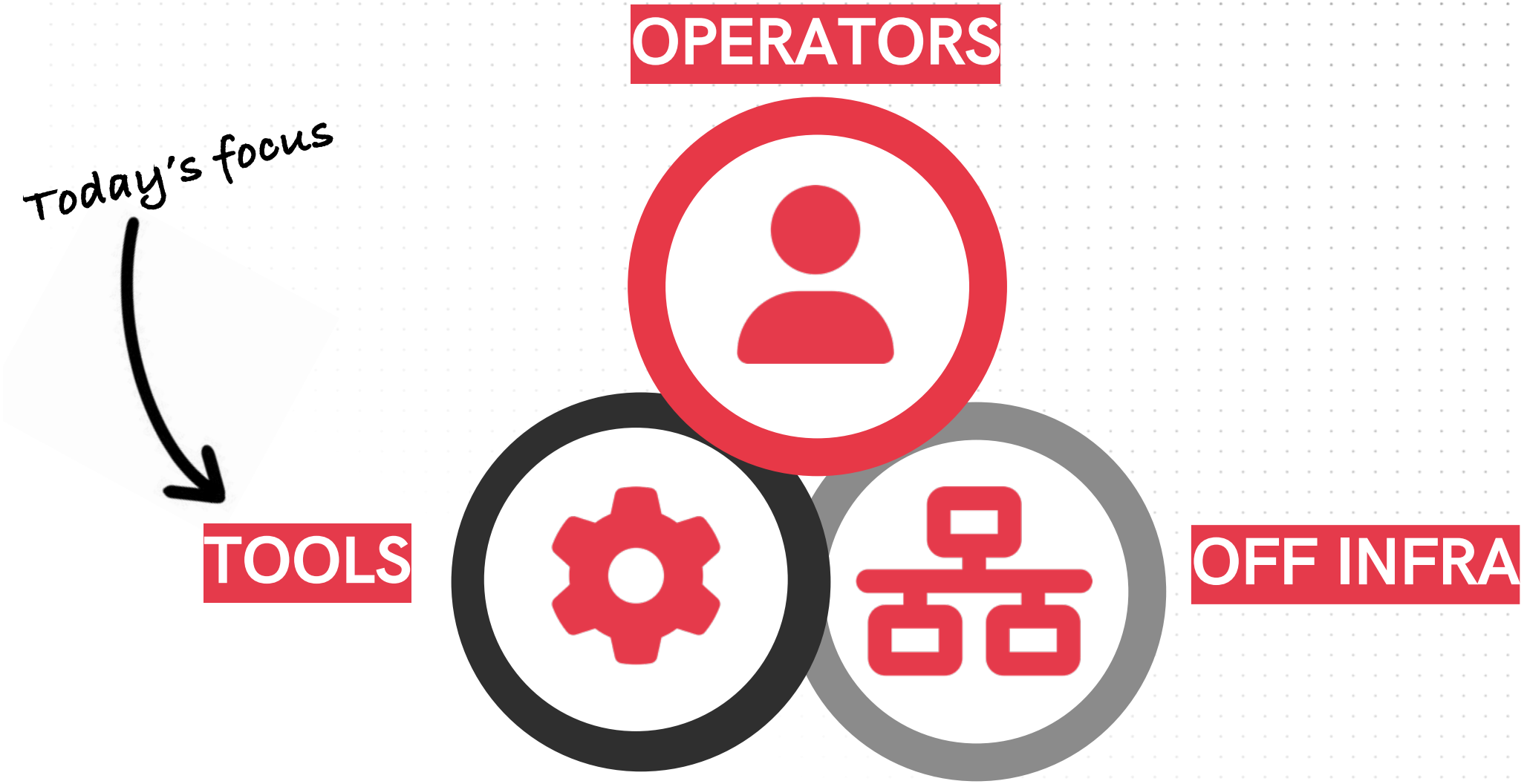
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS


RedBull
ROKT
HONDA
ORACLE
Mobil
Claro
Hard Rock
2

WHAT MAKES A GOOD RACE TEAM?



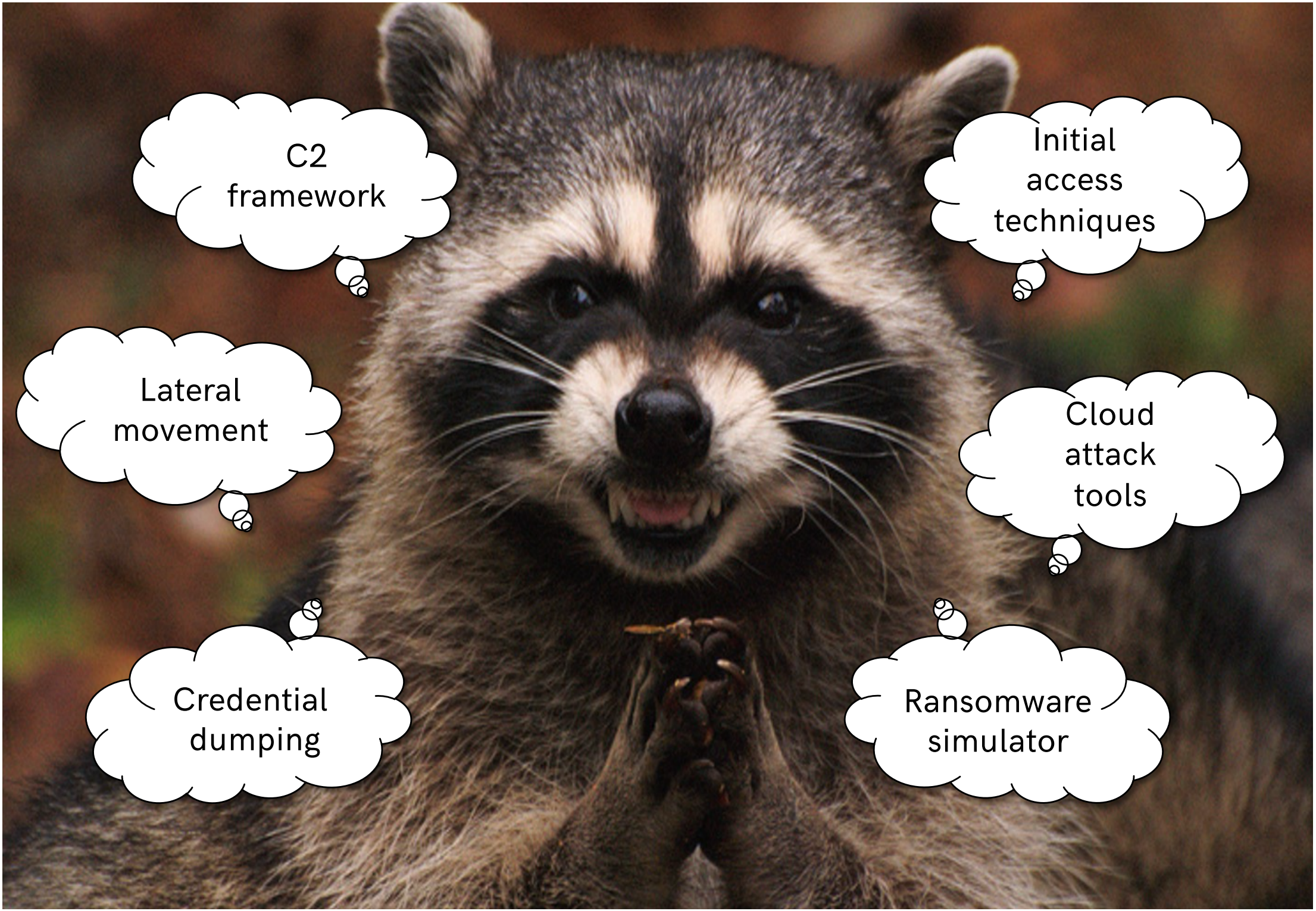
WHAT MAKES A GOOD ~~RACE~~ RED TEAM?




REMEMBER WHEN ... ?
307 eyükkabıyla kadına şiddeti protesto ettiler

TAKEAWAY #1

TIMES HAVE CHANGED. OPEN SOURCE OST JUST DON'T CUT IT ANYMORE


C2 framework
Initial access techniques
Lateral movement
Cloud attack tools
Credential dumping
Ransomware simulator

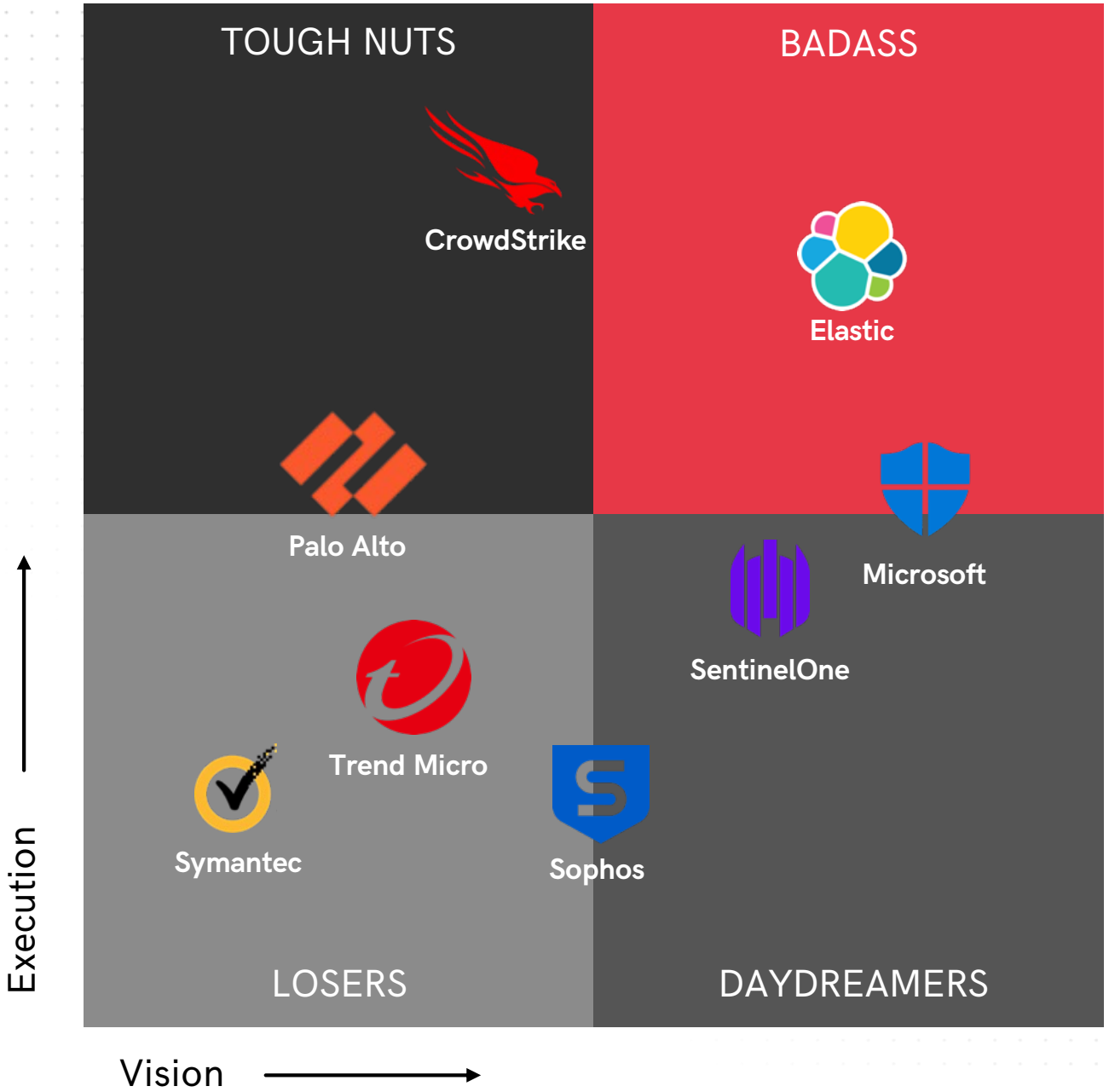
TAKEAWAY #2

A MODERN RED TEAMING ARSENAL IS NOT BUILT BY A LONE WOLF


Team of 5 operators
214 working days
70% billable hours
125 days per TIBER test
= 6 tests per year
Total cost per off dev 120k
2 devs = 240k
40k per test
= 20-40% of test

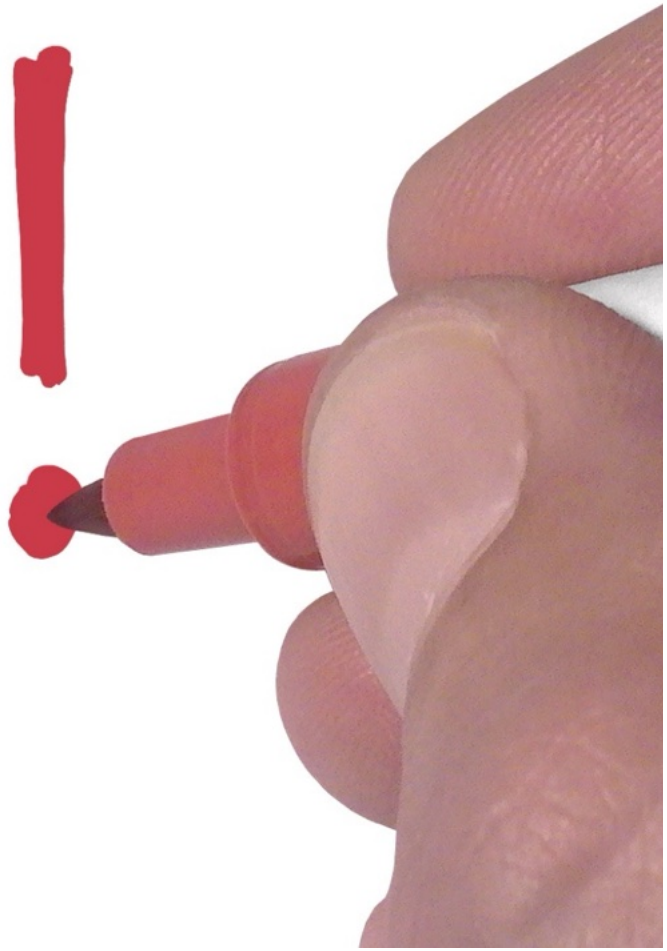

TAKEAWAY #3
RED TEAM TOOLING HAS TO BECOME A VITAL PART OF YOUR BUSINESS STRATEGY

OUTFLANK'S UNOFFICIAL EDR MAGIC QUADRANT



WHAT'S YOUR POINT?

- The tooling ecosystem has changed dramatically
- Make tools a vital part of your red team's strategy
- Litmus test: can your team defeat Elastic EDR?



OUTFLANK

clear advice with a hacker mindset

Stan Hegt
+31 6 1188 5039
stan@outflank.nl
www.outflank.nl/stan