OFFENSIVE SECURITY IN HEALTHCARE

Choosing the Right Engagements & Maximizing Value

William Giles, Head of Adversary Simulation

William.giles@covertswarm.com

LinkedIn: /in/wrgiles

CovertSwarm®

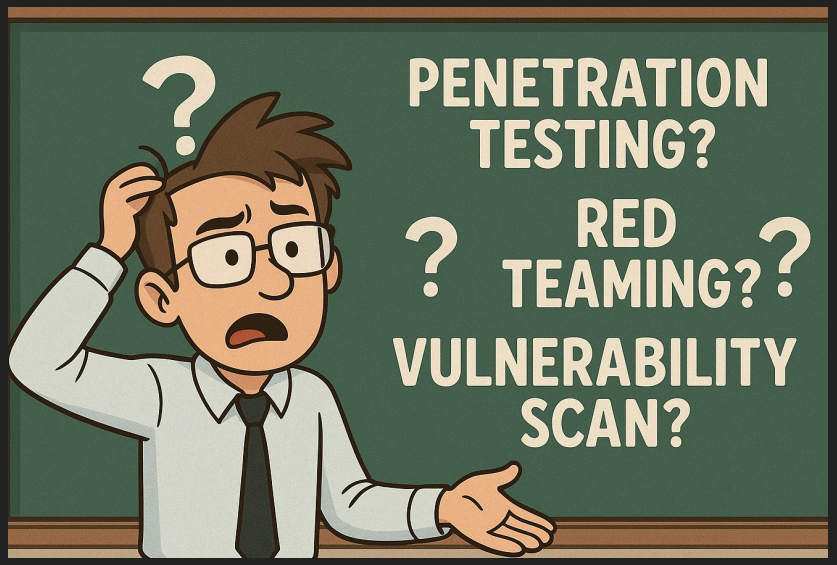
CBEST CREST PEN TEST STAR Intelligence-led PT STAR-FS Intelligence-led PT

OVERVIEW

- What is offensive security?
- Why offensive security matters
- Offensive security maturity
- Types of offensive security engagements
- Choosing the right engagement
- Tips for maximizing value
- Q&A

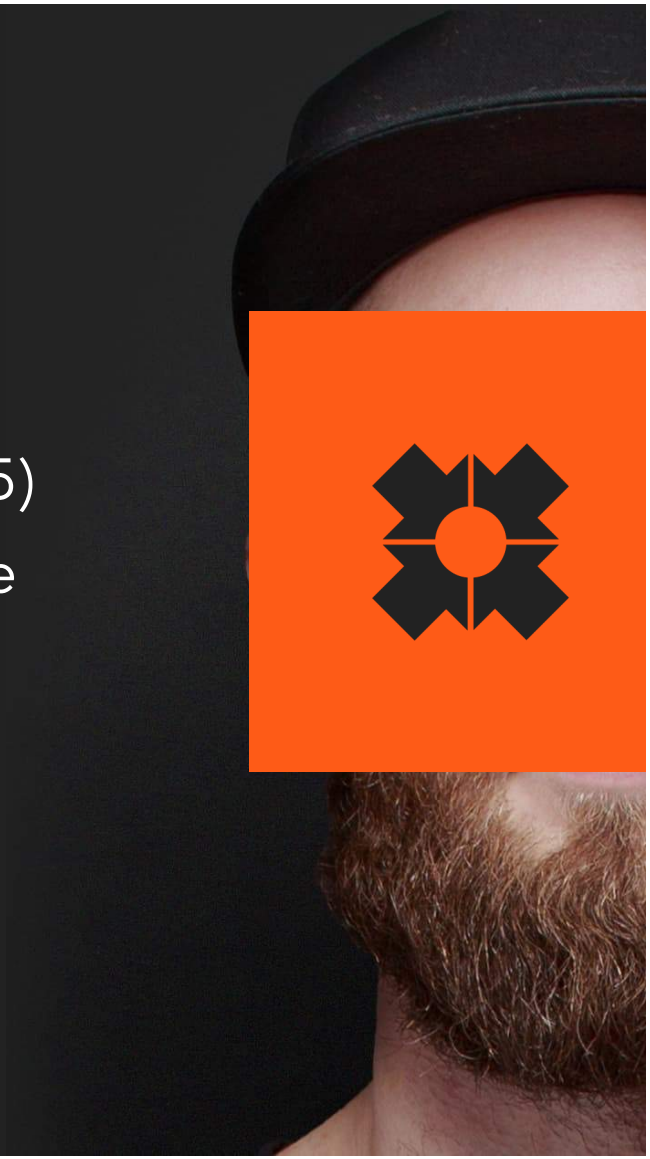
WHAT IS OFFENSIVE SECURITY?

- Offensive security - A proactive approach to cybersecurity that involves simulating real-world attacks to identify vulnerabilities and strengthen defenses
- Overarching term that includes numerous types of tests
- Often referred to as “Red Team”, but Red Team is also a type of offensive security engagement



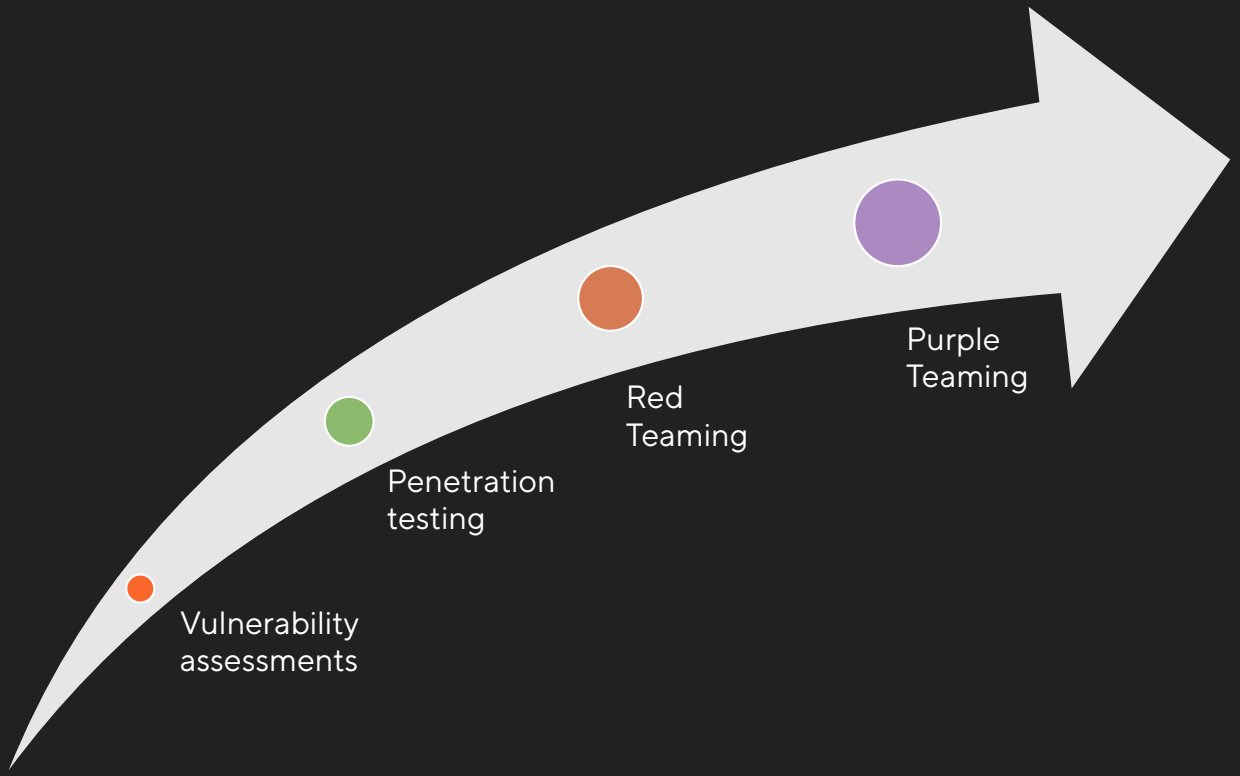
WHY OFFENSIVE SECURITY MATTERS

- Healthcare is a top target for criminals & APTs
- 343 breaches reported in the first half of 2025
- Average healthcare breach cost: $10.22M (2025)
- Breaches disrupt critical care delivery and erode public trust



OFFENSIVE SECURITY ENGAGEMENT TYPES

OFFENSIVE SECURITY MATURITY



OFFENSIVE SECURITY ENGAGEMENT TYPES

Vulnerability Assessments

- Broad, automated scans
- Good for coverage and compliance
- Don't test exploitability
- Lack context

Penetration Testing

- Include exploitation
- Numerous types:
  - Network
  - Web applications
  - Physical security
  - Cloud
  - Mobile
  - Wireless
  - IOT
  - Social engineering*

Red Teaming

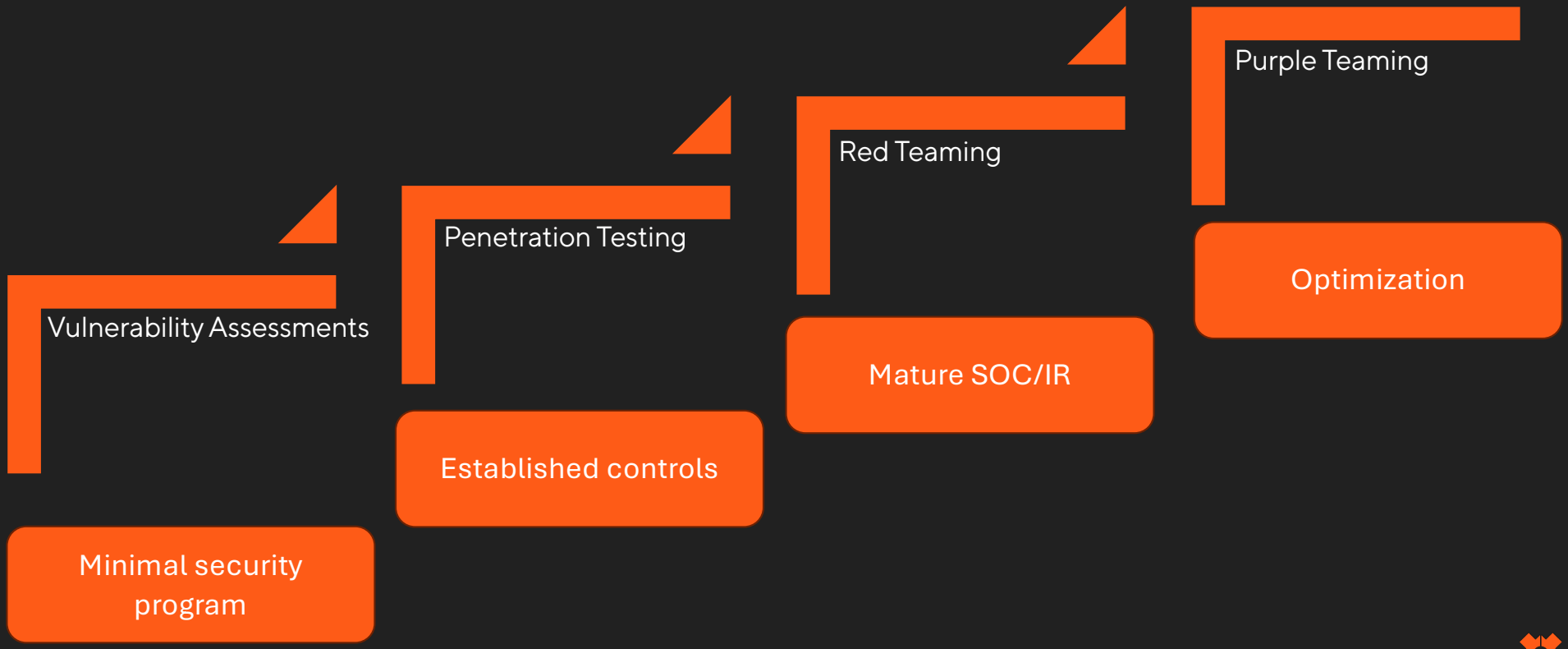
- All assets in scope
- Simulates real threat actors
- Tests people, processes, and technology
- Useful for:
  - Identifying detection gaps
  - Validating alerts
  - Testing incident response
  - Compliance
  - Demonstrating impact

Purple Teaming

- Collaborative
- Useful for tuning sensors

CHOOSING THE RIGHT ENGAGEMENT

CHOOSING THE RIGHT ENGAGEMENT



TIPS FOR MAXIMIZING VALUE

- Work with a partner that specializes in Offensive Security
- Ensure the correct stakeholders are involved in scoping
- Define clear objectives for each engagement
- Include retesting in the Statement of Work
- Develop a multi year testing strategy
- Beware of overly competitive behaviors

SUMMARY

- What is offensive security?
- Why offensive security matters
- Offensive security maturity
- Types of offensive security engagements
- Choosing the right engagement
- Tips for maximizing value

YOU DESERVE TO BE HACKED.

CovertSwarm®