

# THE OPERATOR, NOT THE ORACLE

Why red team tradecraft demands human judgement —  
and how to build AI that amplifies it instead of  
replacing it

LET'S GET  
**REFRACTED**

Refracting risks,  
Revealing solutions

# The AI arms race

## AI-powered detection

ML-driven EDR  
Automated threat hunting  
Behavioral analytics at scale

VS

## AI-enhanced Red Teaming

Automated Recon and enumeration  
Attack path suggestion  
TTP generation and scripting

**The race is happening on both sides. But red teaming isn't about speed.  
It's about thinking like an adversary – and adversaries don't follow playbooks.**

*If AI is changing both offense and defense, the question isn't whether to use it. It's how.*

# Two examples – two lessons

## AI at its best

---

Provided custom binary with hidden credentials  
Discovery in minutes instead of hours

*Lesson: AI is a force multiplier when it handles the grunt work*

## AI at its worst

---

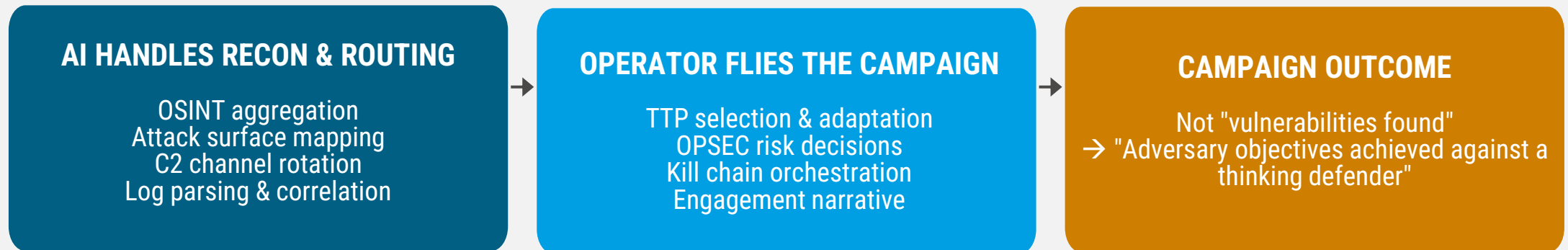
Autonomous agents deployed for scoped reconnaissance  
Probing systems they weren't authorized to touch

*Lesson: AI without boundaries is a liability, not an asset*

**Same tools. Two very different outcomes. The difference is who's in control.**

# AI as tradecraft Co-Pilot

*Every AI-generated TTP recommendation must ship with confidence, rationale, and OPSEC implications.*



## BLACK-BOX OUTPUT

"Send a phishing email to the IT helpdesk"

## CO-PILOT OUTPUT

"Phishing via helpdesk impersonation viable (confidence: 83%)  
– target recently announced a cloud migration on LinkedIn.  
Recommend a fake IT ticket lure. OPSEC note: avoid attachments, their mail filter flags PDFs from new domains.

# Operator-in-the-loop by design

## AI-driven

---

AI picks the attack path  
Operator reviews the conclusion  
Operator is the gate, not the driver  
System optimizes for finding count

## Operator-driven

---

AI surfaces options, operator selects  
Operator adapts the approach  
Operator owns the campaign narrative  
System learns from operator choices

---

### FLOOD THE OPERATOR

100 attack paths, no prioritization  
Alert fatigue → missed opportunities

### ARM THE OPERATOR

Top 5 paths ranked by impact & stealth  
Metric: campaign objectives achieved  
Clarity → better operator decisions

# Transparency = trust

## BLACK-BOX AI

Operator can't assess OPSEC risk  
→ overrides every recommendation

SLOW & DISTRUSTED

VS

## EXPLAINABLE AI

Operator sees reasoning  
→ trusts recommendations → moves faster

FAST & TRUSTED

**If you don't understand why the AI made a recommendation, you can't trust it. And in red teaming, trusting the wrong recommendation can blow the whole operation.**

# Two halves of one weapon system

## THE RED TEAM WEAPON SYSTEM

### AI

Recon, enumeration,  
pattern matching, etc

### OPERATOR

TTP selection, OPSEC,  
adaptation, campaign narrative

You need both. But if you had to pick one to invest in – pick the operator.

# Key Take-Aways

①

## **AUDIT YOUR RED TEAM TOOLCHAIN**

Where is AI making tradecraft decisions for your operators instead of equipping them to make better ones?

②

## **MEASURE CAMPAIGN OUTCOMES, NOT FINDING COUNTS**

Stop counting vulnerabilities. Start measuring: did we achieve adversary objectives against a thinking defender?

③

## **INVEST IN OPERATOR JUDGMENT**

Adversary emulation reps, OPSEC decision drills, cross-team red/blue swaps – the tradecraft skills no model can replicate.

---

**BUILD AI THAT MAKES YOUR RED TEAM  
MORE DANGEROUS, NOT MORE REPLACEABLE.**

# Contact Us

## Speaker contact information

Email: [Thomas.vanderhoydonck@refracted.eu](mailto:Thomas.vanderhoydonck@refracted.eu)

## General contact information

Website: [www.refracted.eu](http://www.refracted.eu)

Email: [info@refracted.eu](mailto:info@refracted.eu)

Phone: +32 (0)3 318 62 40

Adress: Berlaarsestraat 31, 2500 Lier -Antwerp, Belgium

LET'S GET

REFRACTED

Refracting risks,

Revealing solutions.