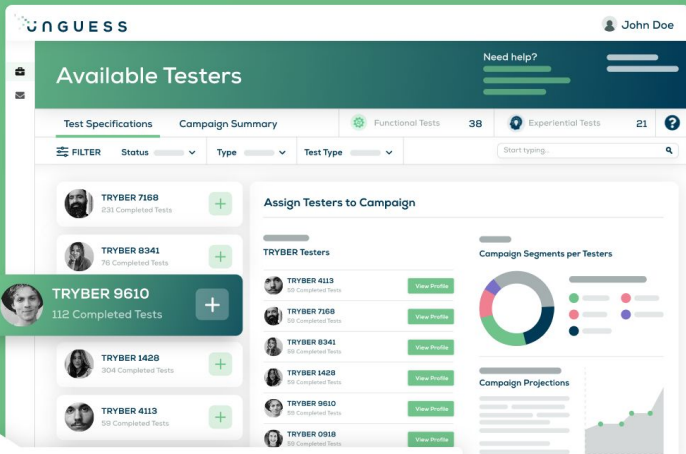


OFFENSIVE SECURITY THAT SCALE
WITH TEAM OF HUMANS + AI AGENTS





**"DNS Hijacking / Subdomain
Takeover" Hacker T122**



**"Remote Code Execution"
Hacker T157**

**UNGUESS's testing platform gives you
the tools to scale Offensive Security**

500+

Customers



200+

European Security
Researchers and AI Agents



€15M

**Euros Raised, from
leading Italian VCs**

Spin-off



**POLITECNICO
MILANO 1863**

UNGUSS Continuous Offensive Security

Improve security by leveraging a **network of security researchers and AI Agents** who collaborate, among themselves and with security teams, to **find vulnerabilities** and **scale offensive security**



POLITECNICO
MILANO 1863

Fintech District



ECCC 
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE



Test better with Teams of Humans + AI Agents

UNGUESS rapidly connects your team to highly skilled specialists from our diverse certified security researchers and a set of AI specialized agents

Internal hacking team



Working side by side with security teams

*Supported by: Testing
Managers, Cybersecurity
Engineers/Leads and
Solution Experts*

Network of Security Researchers



Creativity...

A trusted network of security professionals sharing knowledge, tools, and responsible disclosure to improve systems safely

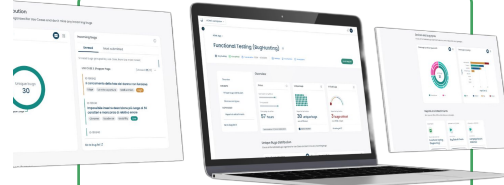
Specialized AI Agents



... and scalability

AI agents automate scale and speed, while security researchers add creativity and judgment to validate and uncover deeper vulnerabilities

UNGUESS Platform



Actionable results

You receive actionable results in real-time on the UNGUESS platform, which can be integrated with your system, such as Jira

The power of Bug Bounty

A full suite of offensive services

Pay-per-result

#1

Continuous penetration test (also called **Bug Bounty programs**) and **VA/PT**

#2

AI / LLM security testing: prompt injection, jailbreaks, tool/plugin abuse, data leakage (RAG), authorization bypass via AI flows, poisoning risks, etc.

#3

Live Hacking Events: a competitive [cybersecurity competition](#) where ethical hackers discover vulnerabilities in your digital assets live, in a controlled and collaborative physical environment.

#4

Vulnerability Disclosure Program (VDP): a policy and process for safe, coordinated reporting of security vulnerabilities.

#5

Social Engineering: phishing simulation, vishing, smishing, credential-harvest resilience, etc.

#6

Fraud Logic Detection: Fraud / business-logic abuse testing, promo abuse, identity theft, account takeover flows, payout manipulation, bot abuse, etc.

#7

Red Teaming augmentation: reinforce an internal/partner red team by adding specialized skills and scalable execution (e.g., extra attack paths, tooling, and coverage) under the same rules of engagement and objectives.

#8

Dark Web and Threat Intelligence: credential leak monitoring (exposure, combos, initial access signals), OSINT/CLOSINT, identify leaked secrets, public repos, employee info exposure, etc.

New challenges for CISOs where UNGUESS Security can help

01.

Increasing threats and **growing costs**



Pay for success: only for certified vulnerabilities we can find

02.

Agile methods and acceleration of **DevOps/AI Building**



Researchers and agents are **always-on** (24/7/365) and can be **integrated with agile** processes

03.

Cyber **talents shortage/Provider Rotation**



A network of hundreds of **fresh-eyes certified professionals**

04.

More **complexity** (AI, API, IoT, etc.) **expanding attack surface**



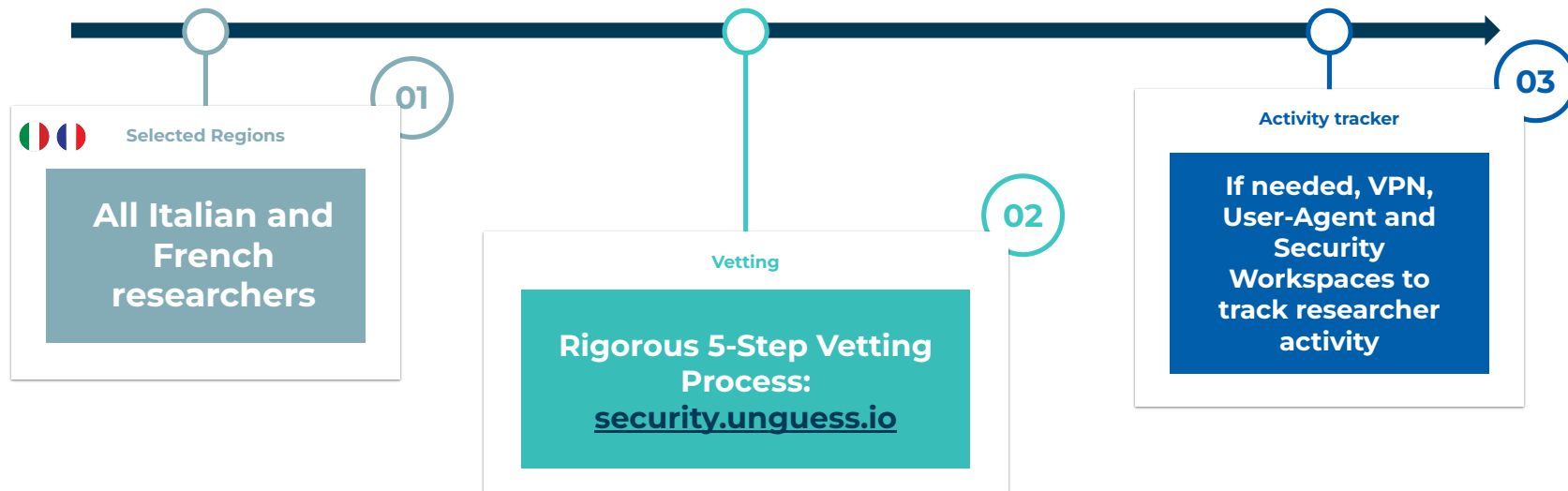
The network of security researchers and specialized agents gives us access to **plenty of different skills**

A network of European certified Security Researchers

231 MODELLO
ORGANIZZATIVO
AI SERVIZI DEL
D. LGS 231/2001

ISO 27001

ISO
9001:2015



CEH

Certified Ethical Hacker

OSCE³

Offensive Security Certified Expert

OSED

Offensive Security Exploit Developer

OSEP

Offensive Security Exploce Pentester

OSWE

Offensive Security Web Expert

OSWE

Offensive Security Web Expert

OSWE

Offensive Security Web Expert

eWPTXv2

Advanced Web Application Penetration Tester

eCPPT

eLearnSecurity Certified Professional

eCPPT

eLearnSecurity Certified Professional Tester

eWPT

eLearnSecurity Web Penetration Tester

eJJPT

eLearnSecurity Junior Penetration Tester

ePISec

API Security Certified Professional

APISec

API Security Certified Professional

PENTEST AGENT

Agent Training

**Human-in-the-Loop
Validation**
(200 UNGUESS Security
Vetted Security
Researchers)



**PENTEST
REPORT**

- 1 Asset & Subdomain Discovery
- 2 Endpoint & API Mapping
- 3 ...
- 4 ...
- 5 ...

- 6 Injection Testing
- 7 XSS & Client-side Exploitation
- 8 ...
- 9 ...
- 10 ...

- 11 Impact & Severity Scoring
- 12 Regression / Retest
- 13 ...
- 14 ...
- 15 ...



Recon
Agent

Recon
Tasks

Attack Vector
Agent

Specialist
Agents

Verification
Agents

Report
Collection Agent

Phase 1:
Intelligent
Reconnaissance

Phase 2:
Attack Planning
& Prioritization

Phase 3:
Controlled Exploitation &
Verification + Reporting

Recon Agent

Attack Vector Agent

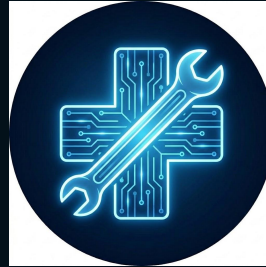
Specialist/Verification/Report Collection Agents

4 AGENTS FROM THE UNGUESS FRAMEWORK



Asset & Subdomain Crawling Agent

Crawls known domains to map the live attack surface - exposed IPs, cloud assets, S3 buckets, and forgotten staging environments linked to the target



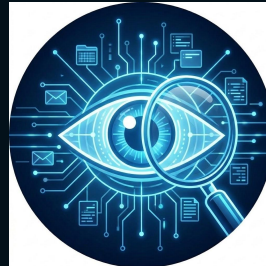
Continuous Adversarial Simulation

Always-on AI agents acting as a persistent Red Team, continuously probing for new exposures, regressions after deployments, and misconfigurations as your attack surface evolves



Asset & Subdomain Discovery Agent

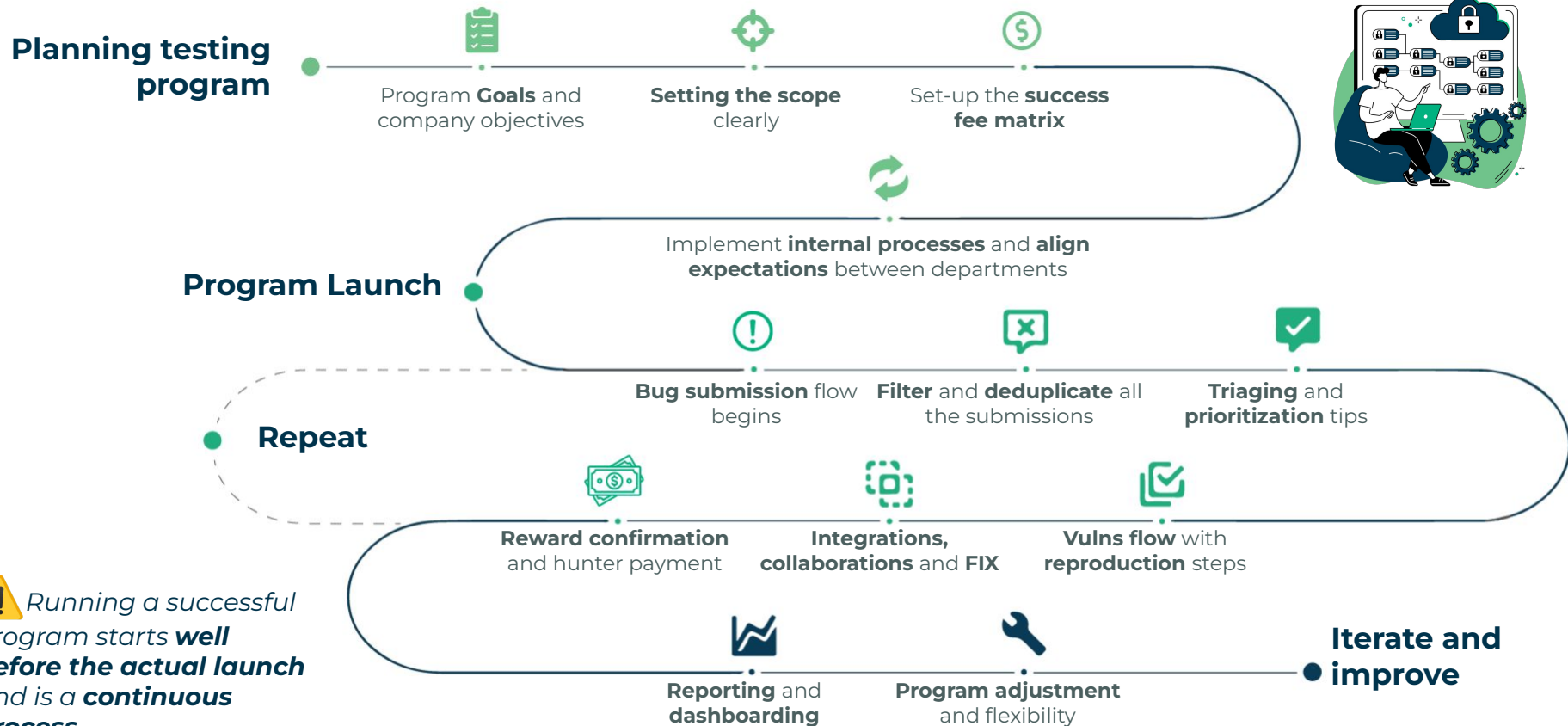
Deep subdomain enumeration via DNS brute-forcing, permutation scanning, and intelligence feeds - uncovering shadow IT and legacy infrastructure that standard crawlers miss (+150% assets discovered vs classic approach)



Client-Side Code Analysis Agent

Parses JavaScript bundles to extract hidden API endpoints, internal routes, undocumented parameters, and hardcoded secrets - feeding them to attack agents for automated exploitation testing

Plan, Launch & **Learn**: The continuous offensive Roadmap



Leading financial institution

Main results

10

Number of **programs** launched in 2 years (**3** always open, **7** time-boxed)

237

Number of **security researchers**

~100

Number of **total vulnerabilities**

2/3 times

€ **saved**



The customer voice



Tap into a widespread set of competencies (from **dozens of different certified EHs simultaneously**)



Scopes/endpoints **steadily under active pentest** help to **decrease the exposure time**



Speed of fixing thanks to the **collaboration between EHs** and **customer sec team**



Defining the scope, bounty caps, etc. **manages to keep costs under control** (and in the end, it **costs less than doing a VA/PT**)

LIVE HACKING EVENT

SEPTEMBER 27 2025

>INITIATE CYBER MISSION_
>EVENT: ROMHACK_2025
>TARGET: CLASSIFIED
>STATUS: LOADING...



Play it!



Where creative minds meet, security evolves

Let's talk.

Scale offensive security and stop guessing your work.



luca.manara@unguess.io



+39 328 6350 983



security.unguess.io