

RO Sovereign Autonomous Cyber Operations Platform

An AI platform for automated cybersecurity assessment and hardening inside a controlled and auditable environment.

ROCyber provides Penetration Testing and Risk Assessment services powered by RO Agentic—an AI system capable of planning tests, conducting assessments, and summarizing vulnerabilities autonomously.

The entire operation runs locally within the organization. System data, vulnerability information, and supporting evidence remain inside the organization. Every action is governed by Scope, Rules of Engagement, and Human Approval.



ONE SCOPE • DEFINED RULES OF ENGAGEMENT • REPRODUCIBLE EVIDENCE



FOUR CORE PLATFORM STRENGTHS

01



SOVEREIGN AI

AI models, data, and testing results remain within Thailand under the organization's control.

02



AUTONOMOUS OPERATION

Plans assessments, selects tools, analyzes results, and adapts within the authorized scope.

03



REPRODUCIBLE EVIDENCE

Delivers Proof of Concept, supporting evidence, and actionable remediation recommendations.

04



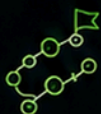
HUMAN-CONTROLLED

Organizations define targets, tools, and permissions—with Human Approval, Audit Logs, and a Kill Switch.

RO AGENTIC'S ADVANCED CAPABILITIES

Beyond signature-based scanning, RO Agentic thinks, plans, and discovers new vulnerabilities within the authorized scope. High-impact actions always require Human Approval.

01



LONG-HORIZON PLANNING

Plans multi-step assessments and connects individual weaknesses into attack chains.

02



AUTONOMOUS REASONING

Forms hypotheses, analyzes results, learns from findings, and replans under expert supervision.

03



ZERO-DAY DISCOVERY

Uses fuzzing and logic analysis to identify previously unknown vulnerabilities and build Proof of Concept within authorized systems.



AUDITABLE THROUGH
AUDIT LOGS • STOPPABLE
WITH THE KILL SWITCH



RO Agentic • Running Locally

PENETRATION TESTING AND RISK IDENTIFICATION

AT AI SPEED, TO PROFESSIONAL PENTEST STANDARDS

RO Agentic handles repeatable reconnaissance, testing, and evidence preparation—allowing specialists to focus on in-depth analysis and interpretation.



ATTACK SURFACE DISCOVERY

Identify assets, services, and access points within the defined scope.



VULNERABILITY VALIDATION

Confirm real exploitability and reduce false positives through evidence-based testing.



RISK RATING & PRIORITIZATION

Prioritize validated vulnerabilities by actual impact and likelihood.

NOT JUST RAW SCAN RESULTS—CLEAR,
VALIDATED RISKS AND ACTIONABLE REMEDIATION PRIORITIES.



r0cyber.com

WHY LOCAL AI?

Penetration testing touches your organization's most sensitive data. R0 Agentic is designed to run inside your environment — no system data, vulnerabilities, or evidence are sent out for external processing.



DATA STAYS ON-PREM

The model and the entire testing process run on your own hardware. System data and findings never leave your network.



NO EXTERNAL EXPOSURE

Can operate fully offline, reducing the risk of leaks through external cloud services or APIs.



COMPLIANCE-FRIENDLY

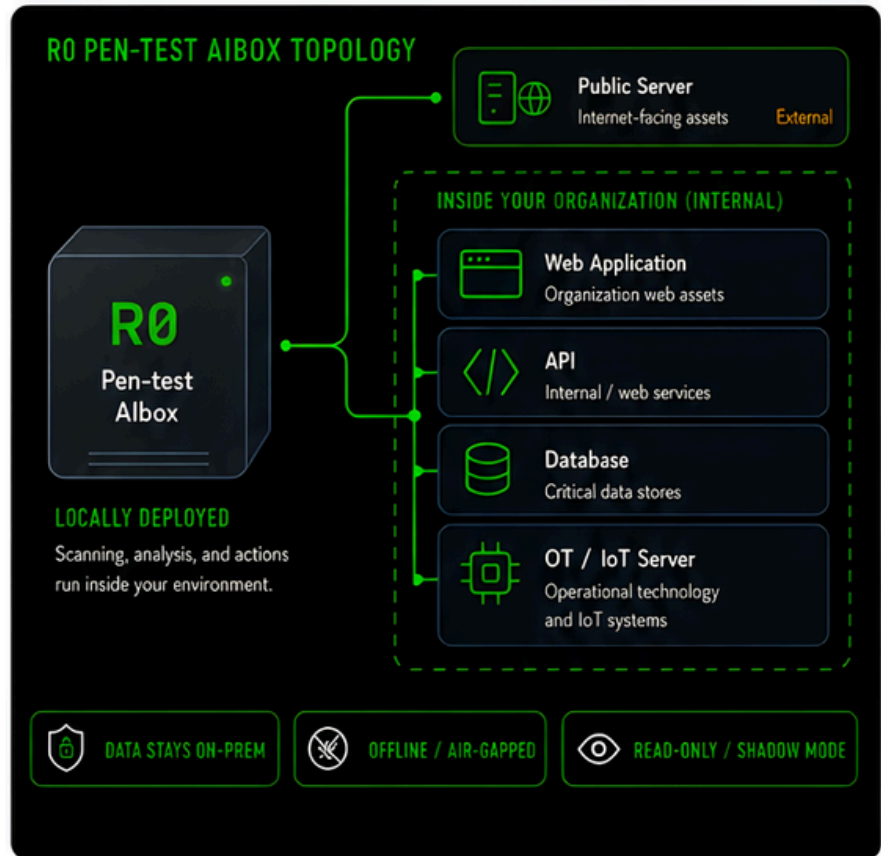
A fit for organizations with data residency and internal data-control requirements (details subject to each organization's actual requirements).



FULL SPEED, FULL CONTROL

Get the speed and coverage of Agentic AI while your organization keeps control of scope — and can stop the run at any time.

R0 PEN-TEST AIBOX TOPOLOGY



HOW IT WORKS



Only owned or authorized systems are tested.
High-impact actions require Human Approval.

SUPPORTED TESTING SCOPES

Start with a clear, measurable scope before expanding to other systems.



EXTERNAL / INTERNAL NETWORK

Network penetration testing from outside and inside your organization.

- ✓ Perimeter & exposed services
- ✓ Internal lateral movement
- ✓ Privilege escalation paths



WEB APPLICATION & API

Web application and API testing following OWASP guidelines.

- ✓ Injection, authZ / authn flaws
- ✓ Business logic abuse
- ✓ API security misconfiguration



CONFIGURATION & HARDENING REVIEW

Review of system configuration and hardening.

- ✓ Misconfiguration & weak defaults
- ✓ Patch & exposure assessment
- ✓ Access control review



RISK ASSESSMENT

Organization-wide risk assessment and prioritization.

- ✓ Threat & impact analysis
- ✓ Attack path mapping
- ✓ Prioritized remediation plan

CYBERGYM BENCHMARK

R0 v4 — CyberGym-Provided 10-Task Subset

10 / 10
TASKS COMPLETED

Base model: Qwen 3.8 • ARV0 6 • OSS-Fuzz 4
Evaluated 31 August 2026

This result covers the CyberGym-provided 10-task subset, not the full 1,507-task Level 1 leaderboard. All 10 tasks reproduced historical vulnerabilities through PoC; they were not direct zero-day discovery tasks.



WHAT YOUR ORGANIZATION RECEIVES

- Executive Summary**
Clear overview of risk posture and priorities.
- Technical Findings + Evidence**
Detailed findings with CVSS, impact, and PoC.
- Prioritized Remediation Plan**
Actionable recommendations and guidance.
- Retest & Verification**
Validation of fixes and residual risk reduction.



Engagement Summary		DETAILS ON THIS REPORT	
Targets: 10 in scope • Scope: external + inside local / office		Critical	Low / Info
3	5	8	4
SEVERITY	PRIORITY	STATUS	STATUS
CRITICAL	SQL Injection — authentication bypass	9.3	✓ confirmed
CRITICAL	Exposed admin panel without MFA	8.6	✓ confirmed
HIGH	S3 bucket misconfigured — public	7.8	✓ confirmed
HIGH	Outdated TLS configuration	7.1	✓ confirmed
MEDIUM	Webinar error messages — info disclosure	5.1	✓ confirmed

LOCAL, AUDITABLE REPORTING



Assess Your System's Risk **Before** Attackers Find the Vulnerabilities

[REQUEST A PENETRATION TEST & RISK ASSESSMENT →](#)



r0cyber.com