

# CyberRecon

## AI-Driven Penetration Testing with Expert Validation

CyberRecon pairs autonomous offensive security — AI agents that explore attack paths and attempt exploitation at machine speed — with CDA security experts who validate every finding, chain the attack paths and translate them into business risk.

The output is proof of exploitation rather than a scanner's list of theoretical vulnerabilities, in reporting built to satisfy SOC 2, ISO 27001, PCI DSS, HIPAA, FedRAMP and cyber insurance requirements — with one remediation retest included.

### WHY CLIENTS BUY THIS NOW

#### A REQUIREMENT

An annual penetration test is mandated by an audit, a customer contract or a cyber insurance carrier, and evidence is due.

#### RELEASE VELOCITY

Code ships weekly. A point-in-time test is stale before remediation finishes, and nothing tests what changed.

#### SCANNER FATIGUE

Reports arrive full of theoretical findings with no proof of exploitability and no way to prioritize them.

### ENGAGEMENT TYPES

Scoped individually or run continuously. Most clients start with external or authenticated testing and expand into continuous coverage.

#### ► External penetration testing

External attack surface, public web applications, APIs, internet-facing infrastructure and authentication portals. Baseline validation and compliance evidence.

#### ► Autonomous continuous testing

Continuous attack surface discovery and exploit validation, rapid retesting after remediation, testing before production releases.

#### ► Cloud penetration testing

AWS, Azure and Google Cloud: IAM privilege escalation, insecure storage exposure, container and serverless weaknesses.

#### ► Authenticated penetration testing

Credentialed application and API testing, role-based access validation, business logic abuse and privilege escalation. Built for SaaS and customer portals.

#### ► API security testing

REST and GraphQL: authentication bypass, broken object level authorization, injection and data exposure.

#### ► DevSecOps security testing

CI/CD pipeline security validation, automated pre-release testing and rapid retesting after code changes.

### WHAT YOU RECEIVE

- **Executive summary report** — business risk and impact, written for leadership, auditors and underwriters.
- **Technical vulnerability report** — findings with exploit reproduction steps and remediation guidance.
- **Proof-of-exploit evidence** — deterministic confirmation that a vulnerability is actually exploitable.
- **Attack path and exploit chain analysis** — how privilege escalation and lateral movement would unfold.
- **Risk-prioritized remediation plan** — ordered by real-world impact, not by raw severity score.
- **One remediation retest** — included, within 60 days of the initial assessment report.

## REPORTING SUPPORTS

| STANDARD / AUTHORITY      | APPLIED TO                                                           |
|---------------------------|----------------------------------------------------------------------|
| SOC 2 and ISO 27001       | Satisfying the annual penetration testing requirement on record      |
| PCI DSS                   | Cardholder data environment testing evidence                         |
| HIPAA                     | Technical evaluation evidence for the Security Rule                  |
| FedRAMP                   | Testing evidence within an authorization program                     |
| Cyber insurance           | Underwriter and renewal evidence of independent testing              |
| Customer security reviews | Vendor due diligence, questionnaires and contractual testing clauses |

## DELIVERY APPROACH

|                                                                                                                                                                                                 |                                                                                                                                                                                          |                                                                                                                                                                                             |                                                                                                                                                                    |                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>1</b><br><b>RECON &amp; MAPPING</b><br>Discover domains, subdomains and exposed assets; enumerate services; fingerprint technology; define scope against real-world threat.<br><b>Step 1</b> | <b>2</b><br><b>AUTONOMOUS EXPLOITATION</b><br>AI-driven discovery across attack paths; injection, authentication, access control, API and business logic abuse testing.<br><b>Step 2</b> | <b>3</b><br><b>EXPERT VALIDATION</b><br>Practitioners confirm exploitability, analyze escalation and lateral movement, identify multi-step chains, assess business impact.<br><b>Step 3</b> | <b>4</b><br><b>REPORTING &amp; REMEDIATION</b><br>Executive and technical reporting, prioritized guidance, remediation support and clarification.<br><b>Step 4</b> | <b>5</b><br><b>RETEST &amp; CONTINUOUS</b><br>One included retest within 60 days; optional continuous testing with quarterly executive risk reviews.<br><b>Elective</b> |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**TIMELINE** Engagements are expected to conclude within 90 days of kickoff, subject to timely access, credentials and authorization. The included retest runs within 60 days of the initial report.

## WHERE AI IS USED – AND WHERE IT IS NOT

- Autonomous platforms explore attack paths and test thousands of exploit scenarios at machine speed — coverage no manual engagement reaches within a testing window.
- Vulnerabilities are confirmed by real proof of exploitation rather than flagged as potential, which removes most false positives before a human ever sees them.
- Continuous testing becomes economical: every release can be tested instead of one assessment a year.
- **Experts validate every result.** Attack chain analysis, business impact and sign-off are human. Client environments and data are not used to train external models.

## WHO BUYS IT

CISO and security leadership · CTO and VP Engineering · CIO · Chief Compliance Officer · Chief Risk Officer · General Counsel · PE operating partners

## IDEAL CLIENT PROFILE

SaaS platforms, customer portals and enterprise applications with meaningful internet-facing exposure or a contractual testing requirement — technology, financial services, healthcare, logistics and government contractors — including DevOps-led teams deploying frequently and PE portfolio companies being diligenced or integrated.

## WHY CDA

► **Proof, not prediction**

Autonomous testing validates exploits with deterministic evidence. A scanner reports what might be exploitable; CyberRecon demonstrates what is.

► **Machine speed, expert judgment**

AI provides the coverage and the volume; practitioners provide the attack chain analysis and the risk narrative a board will accept.

► **Continuous, not annual**

Point-in-time testing ages badly in an environment that ships weekly. Continuous validation tests every release.

► **Retest included**

One remediation validation is part of the engagement, so fixes are proven rather than assumed.

## SCOPE, GUARDRAILS AND RESPONSIBLE AI

Testing begins only with written authorization, test accounts and agreed roles, allowlisting and named contacts. Production testing may generate alerts, logging and temporary performance effects; critical findings are escalated immediately. Internal network, wireless, physical, social engineering, source code review, mobile and DoS testing are out of scope unless added to the SOW. Results are point-in-time.

## Scope it with us.

Engagements are scoped and fixed-fee quoted to your environment. Contact us for scoping, references and a sample deliverable.

833-54-CYBER (833-542-9237)

info@cyberdefenseadvisors.com  
cyberdefenseadvisors.com