CONTINUOUS THREAT EXPOSURE MANAGEMENT (CTEM)

See what an attacker sees. Prove what they could do.

The agentic offensive security catalogue: HiveSec Engine finds what is exposed, proves what is exploitable, and pits a full adversary against your people, process and technology.

STANDING

Continuous Vulnerability Management

Always-on assessment of the external attack surface.

What is exposed, and what has changed.

DEPTH

Penetration Testing

In-depth testing against a defined scope: external, internal or web.

What is genuinely exploitable, and how far it chains.

CONSEQUENCE

Adversary Simulation

Goal-oriented exercise across people, process and technology.

What an adversary achieves, and whether you detect it.

HOW A FINDING BECOMES CONFIRMED

● Confirmed

POTENTIAL FINDING surfaced, unconfirmed → **EXPLOITABILITY** tested against your environment → **EVIDENCE** captured from the target → **ATTACK PATHS** modelled across findings →

PEER REVIEW by separate AI agents → **CONFIRMED** committed as a record

Multiple independent AI agents investigate each potential finding in parallel, and separate AI agents peer-review their conclusions before the finding is committed. What surfaces is confirmed risk, not scanner output.

STANDING · CONTINUOUS VULNERABILITY MANAGEMENT

HiveSec Engine discovers and assesses your entire external attack surface on a continuous schedule.

CONTINUOUS DISCOVERY

The external surface is re-mapped on a daily cadence, so new exposure is caught as it appears, not at the next quarterly scan.

CONFIRMED AND TRACKED

Every finding is confirmed before it surfaces and tracked from first detection to remediation. Findings are managed, not just listed.

DEPTH · PENETRATION TESTING

HiveSec Engine runs an in-depth assessment of a defined scope: external perimeter, internal network, or web application. Each finding is tested for genuine exploitability in the specific deployment, and where findings combine, the platform chains them into attack paths.

ASSESSMENT DEPTH

- L1 Surface enumeration
- L2 Authentication & access control
- L3 Network services
- L4 Application-layer logic
- L5 Service exploitation & validation
- L6 Chained exploit paths

GENUINE EXPLOITABILITY

The test is whether exploitation is achievable against your deployment, not whether a vulnerable version is present. What the platform produces is confirmed evidence of genuine exposure.

FITS THE REQUIREMENT

Depth assessment for a regulatory or insurance requirement, transactional due diligence, or periodic depth above continuous monitoring.

CONSEQUENCE · ADVERSARY SIMULATION

HiveSec Engine runs a goal-oriented adversary simulation across your people, process and technology. You define the attack objective, whether reaching critical data or demonstrating business impact, and the platform pursues it as a real adversary would, taking only the path the objective requires.

RECON
target mapped

→

INITIAL ACCESS
foothold established

→

LATERAL MOVEMENT
reach extended

→

PRIVILEGE ESCALATION
control gained

→

ACTIONS ON OBJECTIVES
impact demonstrated

PREVENTION, DETECTION & RESPONSE

The exercise tests the full defensive posture, not preventative controls alone: whether your processes and people detect and respond while an adversary is actively pursuing objectives.

BOARD-READY

The kill chain is captured as a structured record, mapped against MITRE ATT&CK, and reported in business-impact terms for executive, board, regulator and insurance-market audiences.

ONE PLATFORM UNDERNEATH

The catalogue maps to a CTEM programme: continuous discovery, validation proven by real exploitation, and remediation tracked to closure.

SHARED EVIDENCE

Every service writes to one evidence model. A finding, an attack path and an engagement are the same kind of structured record, held in one place.

LIFECYCLE, NOT SNAPSHOTS

A finding is a persistent object, not a line that reappears on every scan. It keeps a stable identity, status and history, and carries forward until it is closed.

CONFIRMED BY INVESTIGATION

Confirmation works the same way for every service. Each finding is investigated and peer-reviewed by AI agents before it surfaces.

IN YOUR WORKFLOW

Findings are routed to the ticketing and communication systems your teams already use: Jira, Slack, ServiceNow and others, over web and API.

WHO IT'S FOR

ROLE	WHAT THEY GET
Security leaders	An evidence-backed view of your exposure and adversary resilience, in terms that carry to the board.
Security engineers	Confirmed, exploitable findings with evidence and attack paths, routed into existing tooling and tracked to closure.
Boards, regulators & insurers	Penetration testing and adversary simulation that demonstrate resilience for a regulatory, insurance or transactional requirement.
Partners: consultancies & MSSPs	Operate the platform to deliver your own assessment practice. You configure scope and manage the client relationship; the platform executes the methodology.

HOW IT WORKS

01

Scope

Configure the engagement: targets, depth and objectives. Rules of engagement are agreed and documented before work begins.

02

Assess

The platform executes the methodology, discovering the surface, testing exploitability, and chaining findings into attack paths.

03

Confirm

Each finding is investigated and peer-reviewed by AI agents before it surfaces. What reaches you is confirmed risk.

04

Track

Findings land as structured records, routed to your tooling and followed through to remediation.

Speak to us about a HiveSec Engine engagement.

We will walk the catalogue with you and propose the engagement that fits your environment.

Book a demo → hello@hivesec.com

About HiveSec. HiveSec builds offensive-security technology. Our AI agents execute vulnerability discovery, penetration testing and adversary simulation at a scale manual review cannot reach, on one platform with shared evidence and lifecycle tracking. HiveSec LTD, registered in England & Wales · hivesec.com

Assessment scope, depth and objectives are agreed per engagement. The catalogue is growing.