# AI-Augmented Pentesting

Bureau Veritas Cybersecurity offers AI-Augmented Pentesting as a hybrid service for web applications. Autonomous agents expand technical coverage across the target surface, while our pentesters focus on context-driven vulnerabilities, attack chains and the translation of technical findings into organizational risk.

## AI-Augmented Pentesting provides:

### AI scale and human judgment

AI handles repetitive parameter-level testing at scale, freeing our experts for the work where human judgment matters most.

### Human focus on high-value issues

Our pentesters focus on context-driven testing, creativity and organizational understanding to turn findings into real-world impact.

### Zero false positives, preventing false negatives

AI confirms findings with a working exploit. Our experts investigate the promising leads that don't meet that threshold.

## Why hybrid pentesting?

AI is effective at pattern-driven vulnerabilities and large-scale baseline testing. Human pentesters remain essential for context-driven weaknesses, such as business logic abuse, privilege issues, stateful workflows, and multi-step attack paths that depend on how the system is intended to behave.

That is what makes this a true hybrid service. AI performs the systematic sweep, while Bureau Veritas Cybersecurity pentesters shape the scope, investigate near-misses, and turn findings into attack chains that demonstrate real-world impact, with risk prioritization and remediation guidance in your organizational context.

This human-in-the-lead model represents the next evolution of our long-standing expertise in penetration testing.

## How we support you

AI is part of a human-in-the-lead pentest, with scope, oversight, and interpretation led by Bureau Veritas Cybersecurity.

**1 Intake & Scoping**
Define objectives, constraints, access, and the right environment for testing.

**2 Preparation**
Align rules of engagement, test accounts, load limits, and escalation paths.

**3 Execution**
XBOW tests at scale while pentesters focus on business logic, AI near misses and context-driven pentesting.

**4 Reporting**
Deliver validated findings, grouped root causes, and clear remediation guidance.

**5 Advisory call**
Review the results, answer questions, and agree next steps.

## Your challenges

- Pentesting quality is hard to assess: making it difficult to distinguish thorough testing from adequate-but-shallow work, especially for AI-driven testing.
- Time-boxed pentesting can never be exhaustive: even the most experienced pentesters must triage and make choices.
- Using offensive AI responsibly requires understanding its limits and benefits, traceability and human accountability.

## Who is it for?

- Complex scopes with dense user-role logic, high endpoint volume, or layered workflows.
- Development, test, acceptance or production applications and APIs, where rate-limited automated testing can run alongside normal operations.
- Assessments where a fixed timebox would otherwise reduce coverage to sampling rather than depth.

*"AI and experts have the exact opposite strengths and weaknesses. Combine them and you don't add, you multiply."*

**Paul Pols - CTO - Bureau Veritas Cybersecurity**

## Why choose Bureau Veritas

Bureau Veritas Cybersecurity brings 25+ years of pentesting experience to every engagement, with senior review under the four-eyes principle and a strong track record in independent testing and advisory follow-up. For AI-Augmented Pentesting, we combine that pentesting heritage with an exclusive partnership with XBOW, so clients get a hybrid service with wider technical coverage, expert oversight, and findings translated into organizational risk and priority.

## About XBOW

XBOW is an autonomous offensive security platform built for AI pentesting at scale. Its multi-agent architecture deploys agents in coordinator, worker, attacker and validator roles, with non-destructive validation and a zero-false-positives approach. XBOW ranked #1 on the HackerOne leaderboard in August 2025. All assessment data and AI models are hosted in the EU by default.

**Interested?**

Contact us today:

cybersecurity@bureauveritas.com
cybersecurity.bureauveritas.com

***AI scale. Human judgment. Assured outcomes.***