

Raptoric Launches Security Testing for High-Risk AI Systems Under the EU AI Act

Cybersecurity firm Raptoric has launched a security testing service for high-risk AI systems, covering adversarial, robustness and cybersecurity testing.

ZAGREB, CROATIA, June 13, 2026

/EINPresswire.com/ -- Global

[cybersecurity](#) firm [Raptoric](#) has launched a security testing service for artificial intelligence systems, helping organizations meet the robustness and cybersecurity requirements the [EU AI Act](#) places on high-risk AI.



The AI Act (Regulation (EU) 2024/1689) requires high-risk AI systems to achieve appropriate levels of accuracy, robustness and cybersecurity, and to be resilient against attempts to manipulate their behavior. Meeting that standard calls for technical testing beyond conventional software security assessment, including adversarial testing, data and model integrity review, and resilience against attacks such as prompt injection, data poisoning and model evasion.



High-risk AI has to be demonstrably robust and secure, and that is a technical result you test for, not a policy you write."

Marko Lukan

The timeline has recently shifted. Under the Digital Omnibus on AI, agreed by EU institutions in May 2026 and expected to be formally adopted during 2026, the

compliance deadline for standalone high-risk AI systems moves from August 2026 to 2 December 2027, with high-risk AI embedded in regulated products moving to 2 August 2028. Raptoric advises organizations to treat the additional time as a window to build security testing into their AI systems rather than as a pause.

"The deadline moved. The engineering did not get any easier," said Marko Lukan, Security Consultant at Raptoric. "High-risk AI has to be demonstrably robust and secure, and that is a technical result you test for, not a policy you write. The companies that use this window to build and document that testing will be ready. The ones treating December 2027 as a distant problem

will not."

Raptoric's AI security testing covers adversarial and robustness testing, review of training data and model supply chains, security assessment of the infrastructure around deployed models, and reporting structured to support AI Act conformity work. The service also addresses operational risk beyond regulatory compliance, including the risk that AI systems can be manipulated, degraded or exploited once in production.

About Raptoric

Raptoric is a global provider of technical cybersecurity services. The company provides penetration testing, AI security testing, virtual CISO services, incident response, and regulatory-aligned security testing for frameworks including the EU AI Act, NIS2, DORA and the Cyber Resilience Act. More information is available at raptoric.com.

Marko Lukan
Raptoric
[email us here](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/919493615>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.