Horizon3.ai Launches Rapid Response to Secure the Era of AI-Powered Attacks

Wednesday 3 June, 2026

Related Sectors:

Computing & Telecoms ::

Related Keywords:

IT Security :: Artificial Intelligence :: Cyber Security ::

Scan Me:

Rapid Response gives defenders clear vulnerability prioritization as AI shrinks exploit windows to less than 24 hours.

London, 3 June 2026 — Horizon3.ai, the AI-native proactive security leader, announced Rapid Response , a new capability that helps organisations identify, prioritise, and respond to emerging threats in an era of AI-driven vulnerability discovery and exploit development. As exploit windows continue to shrink, organisations are struggling to determine which threats represent genuine business risk before attackers can weaponise them. Rapid Response helps security teams close the exploit window faster by validating exposure, prioritising remediation, and verifying fixes.

From Vulnerability Overload To Actionable Priorities

Security teams are inundated with vulnerability disclosures, threat intelligence feeds, exploit chatter, and vendor advisories, all demanding immediate attention. While tens of thousands of new vulnerabilities are disclosed each year, only a small fraction are actively exploited. Across more than 250,000 NodeZero security assessments, Horizon3.ai has consistently found that exploitability, not vulnerability count, is what matters most. The challenge is no longer visibility. The challenge is determining which threats are actually exploitable and require immediate action.

Rapid Response helps organisations cut through the noise by answering the questions that matter most during emerging threat events: Are we actually at risk? Which assets are exposed? What action should we take first? Did our mitigation efforts work? And can we demonstrate risk reduction to leadership?

AI Is Accelerating the Attacker Timeline

As AI-driven vulnerability discovery accelerates and exploit windows continue to shrink, organisations need better signal, not more noise. Rapid Response is Horizon3.ai's answer to that challenge.

Horizon3.ai's Attack Team continuously monitors and evaluates newly disclosed vulnerabilities based on factors such as attacker interest, how widely affected technologies are used, ease of exploitation, and the likelihood that attackers will begin using them at scale. This helps organisations focus on the threats that pose the greatest real-world risk instead of reacting to every new headline vulnerability.

“As a CISO, can your team handle responding to 1 CISA KEV per quarter? What about 1 per month? Per week? Per day?” said Snehal Antani, CEO and co-founder of Horizon3.ai. “With Mythos compressing the time and effort to exploit code, we should anticipate a CISA KEV tsunami in the second half of 2026, which is why we prioritised Rapid Response.”

Faster Answers When Every Hour Matters

Rapid Response addresses this challenge by combining emerging threat intelligence, exposure validation, and insights from the NodeZero® AI-Native Proactive Security Platform to help security teams move from uncertainty to action faster. It delivers early warnings on confirmed exploit risks, targeted validation tests, and remediation guidance, often before vulnerabilities are added to the CISA Known Exploited Vulnerabilities catalog. When high-risk vulnerabilities emerge, Horizon3.ai develops production-safe, repeatable validation tests, frequently within hours, using a combination of AI-assisted research, expert human analysis, and real-world attacker tradecraft.

"The pace of modern threats is exposing the limits of traditional vulnerability response. Security teams can no longer afford to spend days coordinating assessments, remediation plans, and validation efforts when attackers move in hours. Rapid Response helps organisations accelerate that process and respond with greater confidence when time matters most," added Dan Bird, Field Chief CTO EMEA at Horizon3.ai.

With Rapid Response, organisations receive a personalised view of their exposure, guided remediation workflows, and progress tracking from discovery through resolution. Security teams can identify which assets are exploitable, potentially at risk, mitigated, or not exploitable; safely validate mitigations in production environments; track remediation progress over time; and demonstrate measurable risk

reduction and response timelines.

The principle behind Rapid Response is simple: focus on what attackers can actually exploit. As AI accelerates vulnerability discovery and exploit development, security teams need a faster way to separate real risk from noise, verify exposure, and prove risk reduction. Rapid Response is the signal in the vulnerability noise, helping organisations hack, fix, verify, and repeat on-demand against the threats that matter most.

Learn more about Rapid Response:
https://horizon3.ai/intelligence/blogs/exploit-window-shrinking-rapid-response/

About Horizon3.ai

Horizon3.ai, the AI-Native Proactive Security Company behind NodeZero®, shifts the advantage from attackers to defenders by giving organisations the power to fight AI with AI. NodeZero, the World's Best AI Hacker™, autonomously tests your defenses at machine speed, safely finds and prioritises exploitable attack paths, instantly verifies fixes, and drives a continuous hack, fix, verify loop. More than 5,500 organisations including the NSA, CISA, Fortune 100 giants, and major healthcare providers trust Horizon3.ai to prioritise what matters and for security you can prove.

Follow HORIZON3.ai on LinkedIn
and X.

Further information: Press contact: Kyrk Storer - press@horizon3.ai, Web: www.horizon3.ai

PR Agency: euromarcom public relations GmbH, Web: www.euromarcom.de, Email: team@euromarcom.com

Company Contact:

_

news aktuell

E. desk@newsaktuell.de
W. https://www.newsaktuell.de/

View Online

Newsroom: Visit our Newsroom for all the latest stories:
https://www.newsaktuell.pressat.co.uk