Horizon3.AI Europe GmbH

26.03.2025 – 14:19 Uhr

Horizon3.ai Releases 2025 Cybersecurity Insights Report: Key Findings from Over 50,000 NodeZero® Pentests

London (ots) -

Keith Poyser, Vice President for EMEA: "This report offers a groundbreaking analysis based on real-world cyberattack techniques conducted at organisations across the globe, delivering invaluable insights."

Horizon3.ai, a global leader in offensive security, today released its 2025 Cybersecurity Insights Report, revealing the common security gaps organisations struggle to close. By analysing exploit trends from 50,000 NodeZero® autonomous security tests run in 2024, along with insights from a survey sample of nearly 800 security leaders and practitioners, the report presents clear evidence of how current security strategies are failing, and what organisations must change to stay ahead of evolving threats.

Horizon3.ai defines offensive security as using real-world attacker techniques to identify and exploit weaknesses across IT environments—proving what's truly at risk. Unlike passive security, which relies on layered defences with unverified effectiveness, NodeZero autonomously conducts safe, full-scale tests that demonstrate exactly how attackers could compromise critical systems. The result: clear, actionable proof that enables teams to find, fix, and verify vulnerabilities—before adversaries strike.

Horizon3.ai highlights key findings from the report:

- **Vulnerability Scanning Falls Short** – Despite 98% of organisations using vulnerability scanning, only 34% find it highly effective due to false positives that hinder teams from focusing on real risks.
- **Credential-Based Attacks Remain a Major Risk** – NodeZero successfully performed credential dumping in over 28,000 cases, demonstrating the widespread risk of weak credential practices and policies.
- **Patch Management Delays Leave Systems Exposed** – Over half of practitioners (53%) and more than a third of security leaders (36%) admit to delaying patches due to operational constraints, leaving critical vulnerabilities open.
- **Known Vulnerabilities Remain Unpatched** – NodeZero exploited 229 known vulnerabilities nearly 100,000 times in customer environments, demonstrating that many organisations struggle to remediate even widely recognized threats.

"Security isn't about reacting—it's about outpacing your adversary," said Snehal Antani, CEO & Co-Founder of Horizon3.ai. "Too many organisations still confuse compliance for security, falling back on outdated assumptions and annual testing cycles. This report shows what modern defenders already know: you have to think like an attacker, validate like an operator, and build a security program that stands up to real-world pressure."

Why Offense-Driven Security Is the Only Way Forward

These aren't isolated problems—they reflect a broader pattern the report lays bare. Across nine key themes, it shows that organisations continue to rely on point-in-time testing, noisy tools, and risk models built on assumptions rather than proof.

Each section exposes a recurring failure, from vulnerability overload and delayed patching to ineffective pentests, cloud misconfigurations, and especially credential weaknesses. Fixing these issues requires more than remediation; it demands continuous visibility into identity, access, and privilege exposure.

The takeaway: only an offense-driven approach that continuously tracks readiness and validates defences while leveraging deception, detection, and real-world attacker perspectives can expose and eliminate the gaps attackers rely on.

"This report is a reality check for security teams," said Stephen Gates, Principal Security SME at Horizon3.ai. "It doesn't just highlight where defences are failing, it points to a better path forward. If you're still relying on assumptions, static tools, or annual tests, this data makes it clear: it's time to evolve. Offensive security isn't a nice-to-have—it's the strategy that separates the resilient from the exposed."

The State of Cybersecurity in 2025: Data-Driven Insights from Over 50,000 NodeZero® Pentests is available now. Explore the root causes behind today's most persistent security failures—and learn how an offense-driven approach is helping organisations finally close the gaps attackers rely on.

Download the full report today.

About Horizon3.ai and NodeZero: Horizon3.ai provides a cloud-based platform, NodeZero, enabling organisations and public authorities to run production safe self-attacks on their IT infrastructure to assess their cyber resilience through penetration testing (pentesting). Thanks to its cloud model, the platform offers affordable, regular autonomous pentesting, making it accessible from small to mid-sized, to large enterprises. Horizon3.ai continuously monitors the cybercrime landscape to ensure that newly discovered vulnerabilities are swiftly integrated into the cloud system. NodeZero not only identifies security flaws but also offers tailored recommendations for remediation. Through this platform, Horizon3.ai helps organisations meet rising regulatory demands for cyber resilience in Governance, Risk & Compliance (GRC), with guidelines recommending an internal self-attack at least once a week.

Trademark notice: NodeZero is a registered trademark of Horizon3.ai

Further information:

Horizon3.AI Europe GmbH, Prielmayerstrasse 3, 80335 Munich, Web: www.horizon3.ai

PR Agency
euromarcom public relations GmbH, www.euromarcom.de, team@euromarcom.de