20.05.2025 – 10:51 Uhr

Horizon3.ai Gains FedRAMP High Authorisation, Delivering on Its Commitment to Secure the Public Sector

San Francisco (ots) -

Horizon3.ai, the global leader in offensive security, today announced it has gained Federal Risk and Authorisation Management Program (FedRAMP®) High Authorisation, unlocking the ability to support even the most security-sensitive federal missions. This milestone fulfils Horizon3.ai's previously announced commitment to bring proof-based security to government agencies operating at the highest levels of compliance and risk exposure.

Horizon3.ai's newly authorised platform, NodeZero Federal™, is now available to federal agencies under the FedRAMP High baseline. Built upon the proven commercial version of the NodeZero® Offensive Security Platform, NodeZero Federal™ is designed specifically to meet the heightened security and compliance demands of government environments. With this authorisation in place, Horizon3.ai becomes the first and only cybersecurity vendor authorised to deliver continuous, autonomous pentesting within this strict regulatory framework.

"We built NodeZero to help defenders find and fix vulnerabilities and weaknesses before attackers exploit them—and with the FedRAMP High authorisation, we're now able to proactively secure critical federal systems," said Snehal Antani, CEO and Co-founder of Horizon3.ai. "Our roots are in National Security, and with cyber warfare evolving at an unprecedented pace, we're committed to improving the cyber resilience of the nation's digital infrastructure, with support for Secret and Top Secret systems as our next major focus areas."

This authorisation builds on Horizon3.ai's success with Federal partners, such as the NSA Cybersecurity Collaboration Center (CCC) program. As part of CCC, Horizon3.ai powers the NSA's Continuous Autonomous Penetration Testing (CAPT) program, where Defense Industrial Base (DIB) suppliers use NodeZero to act as nation-state-level adversaries, identify and prioritise real attack paths, and continuously validate their defences.

"Through our FedRAMP High authorisation, federal agencies and key suppliers can assess and improve their cybersecurity stance, ensuring that their limited resources are focused on the issues that matter most," said Keith Poyser, Vice President for EMEA. "This enables agencies to systematically find, fix, and verify the mitigation of CISA Known Exploitable Vulnerabilities (KEVs) across their systems, ensure their security operations centres are effectively stopping attacks, and fine-tune their security tools. In the realm of cybersecurity, a strong offense is essential for building effective defence, a principle that our US Federal clients deeply understand."

NodeZero Federal helps agencies streamline compliance with key cybersecurity mandates, including NIST SP 800-53—the foundational control framework behind FedRAMP—as well as evolving OMB policies and Executive Orders that require Zero Trust architecture, Cybersecurity Maturity Model Certification (CMMC) 2.0 for supply chain assurance, and participation in Continuous Diagnostics and Mitigation (CDM) programs.

For more information about Horizon3.ai's NodeZero Federal™ and its FedRAMP High capabilities, visit their website.

Follow Horizon3.ai on LinkedIn and X.

About Horizon3.ai and NodeZero: Horizon3.ai provides a cloud-based platform, NodeZero, enabling organisations and public authorities to simulate 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 pentesting, making it accessible to mid-sized companies. 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.

Contact:

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

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