HORIZON3.ai
~~TRUST BUT~~ VERIFY

Horizon3.AI Europe GmbH

12.11.2024 – 09:01 Uhr

Horizon3.ai Launches NodeZero™ Kubernetes Pentesting, Empowering Organisations to Protect Critical Infrastructure

Horizon3.ai Launches NodeZero™ Kubernetes Pentesting, Empowering Organisations to Protect Critical Infrastructure

- **Shift in Cybersecurity Towards Offensive-Based Assessments to Secure Kubernetes Clusters.**
- **CEO Snehal Antani: "It's about putting organisations into a 'wartime readiness' stance."**

London, November 12 2024 – Horizon3.ai, a global leader in autonomous security solutions, proudly announces the release of NodeZero™ Kubernetes Pentesting, a powerful new capability available to all NodeZero users. This solution enables organisations to identify and exploit vulnerabilities from an attacker's perspective, uncovering potential security gaps that could jeopardise their entire infrastructure.

Kubernetes has become foundational to modern environments, offering flexibility to scale containerised applications. However, as adoption of managed Kubernetes distributions like AWS Elastic Kubernetes Service (EKS), Google Kubernetes Engine (GKE), and Azure Kubernetes Service (AKS) grows, the risks from complex and distribution-specific weaknesses increases as well. NodeZero's offensive approach prioritises real-time security testing at the runtime level, revealing the "blast radius" attackers could achieve by chaining Kubernetes-specific vulnerabilities with cloud and on-premises infrastructure weaknesses.

Protecting Kubernetes as Rigorously as any Core System

"With Kubernetes operating as essential infrastructure, security teams must defend it as rigorously as any core system," said Snehal Antani, CEO and Co-Founder of Horizon3.ai. "NodeZero Kubernetes Pentesting goes beyond surface checks—showing exactly how attackers can exploit weaknesses in real time. This is about putting organisations in a 'wartime' stance, enabling them to see the true paths of attack and proactively harden their defences against evolving threats."

Keith Poyser, Vice President for EMEA at Horizon3.ai adds: "We continuously expand NodeZero with essential new features and enhancements that enable companies and organisations to actively assess their cyber resilience. Following the launch of NodeZero Tripwires, Cloud Penetration Testing, Rapid Response Service, and Phishing Impact Testing earlier this year, we are now introducing another significant feature with NodeZero Kubernetes Pentesting."

NodeZero Kubernetes Pentesting differentiates itself through advanced runtime security testing and ease of deployment, allowing organisations to achieve the continuous security assurance demanded by today's threat landscape. Unlike traditional security tools focused on compliance or control plane analysis, NodeZero tests in real time, uncovering vulnerabilities like container escapes and RBAC misconfigurations that attackers exploit to move laterally, escalate privileges, and compromise underlying infrastructures.

The release underscores a shift in cybersecurity toward offensive-based assessments that employ adversarial techniques. Traditional compliance-driven assessments often miss critical gaps that attackers could exploit, leaving organisations exposed. With NodeZero's use of real-world tactics, techniques, and procedures (TTPs) that mimic attacker behaviour within Kubernetes environments, security teams can prioritise the most pressing threats and address exploitable vulnerabilities before they become gateways for adversaries.

Designed for any Kubernetes distribution, including EKS, GKE, and AKS, NodeZero's pentesting capabilities provide advanced protection across both cloud and on-premises clusters. This solution underscores Horizon3.ai's commitment to proactive, high-impact cybersecurity innovation, helping organisations navigate and secure the complexities of Kubernetes at scale.

About Horizon3.ai and NodeZero: Horizon3.ai offers a cloud-based platform called NodeZero, enabling organisations and government agencies to conduct self-assessments of their IT infrastructure to verify their cyber resilience (also known as penetration tests or pentests). Thanks to the cloud-based model, the costs are low, making regular pentesting affordable even for medium-sized companies. Horizon3.ai continuously monitors the cybercrime landscape to immediately address emerging vulnerabilities through the cloud. NodeZero not only identifies security gaps but also provides concrete recommendations for remediation. With this platform, Horizon3.ai helps organisations and government agencies meet the growing regulatory requirements for cyber resilience in the areas of "Governance, Risk & Compliance" (GRC), which recommend conducting a self-assessment at least weekly.

Trademark notice: NodeZero is a trademark of Horizon3.ai

Further information: Horizon3.AI Europe GmbH, Sebastian-Kneipp-Str. 41, 60439 Frankfurt am Main, Web: www.horizon3.ai

PR Agency: euromarcom public relations GmbH, Tel. +49 611 973150, Web: www.euromarcom.de, Email: team@euromarcom.de

- - - -