Sec4good

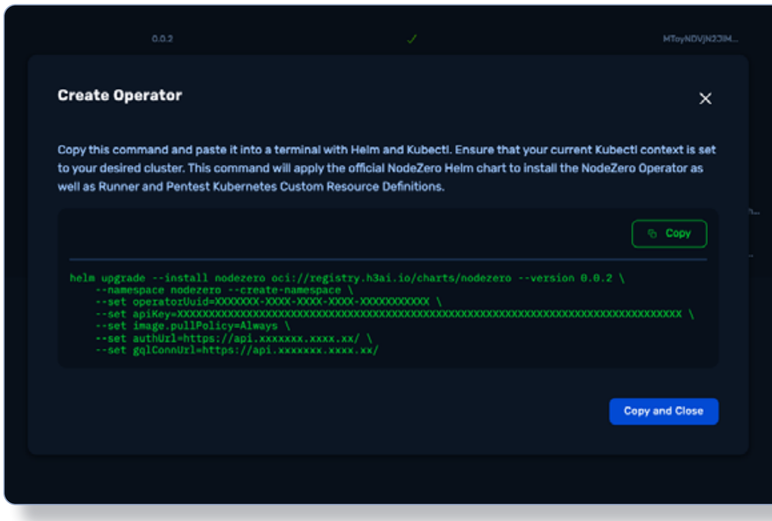
HORIZON3.ai

~~TRUST BUT~~ VERIFY

NodeZero for Kubernetes

NodeZero's Kubernetes Pentesting is the first fully autonomous security solution designed to deploy directly inside Kubernetes clusters. It provides real-time, continuous testing that focuses on runtime vulnerabilities, unlike traditional tools that focus only on control plane analysis.

This enables organizations to prioritize actual risks by demonstrating how attackers can exploit Kubernetes weaknesses, regardless of whether the environment is on-premises, hybrid, or cloud-based.



Key Features

Deploys Seamlessly: NodeZero deploys directly into Kubernetes clusters using Kubernetes Operators, allowing teams to quickly deploy with a simple *kubectl* command. It eliminates complex setup, enabling immediate pentesting inside Kubernetes clusters with minimal effort.

Continuous Testing: With a one-time setup of NodeZero Runners, users can effortlessly enable continuous testing of Kubernetes environments. Once deployed, these Runners allow teams to easily re-deploy tests anytime, keeping up with the evolving nature of containerized environments and ensuring consistent security without the need for repeated manual setup.

Exploits Runtime Vulnerabilities: NodeZero actively exploits vulnerabilities at runtime, showing the real-world impact of container escapes, RBAC misconfigurations, and privilege escalation risks. It goes beyond detecting issues or potential vulnerabilities by proving their exploitability.

Supports All Kubernetes Distributions: NodeZero works seamlessly with all Kubernetes distributions, including managed environments like EKS, GKE, and AKS. It ensures full coverage across multi-cloud or hybrid environments, no matter the platform.

Automatically Prioritizes Risks: NodeZero ranks vulnerabilities based on their severity and exploitability, helping teams focus on fixing critical issues first. It reduces the manual workload by handling threat research and prioritization automatically.

Key Differentiators

First Fully Autonomous Pentesting for Kubernetes: NodeZero is the only solution that is deployable in a Kubernetes cluster and can autonomously test Kubernetes clusters in real-time, continuously identifying exploitable vulnerabilities without requiring human oversight.

Real-World Exploits, Not Just Control Plane Analysis: While most tools focus on control plane misconfigurations, NodeZero identifies vulnerabilities that occur during runtime. By actively exploiting vulnerabilities and targeting weaknesses, NodeZero ensures that security is not just theoretical but practical, giving security teams a clear picture of how attackers can compromise their systems and not just flagging theoretical risks.

Cross-Platform Exploit Chaining: NodeZero uniquely identifies and exploits vulnerabilities not just in Kubernetes itself, but also in the underlying infrastructure (cloud or on-prem). For example, it demonstrates how attackers could combine Kubernetes and cloud-specific weaknesses (e.g., AWS or Azure vulnerabilities) to achieve a bigger impact across the organization.

Why It Matters Now

With Kubernetes rapidly becoming the backbone of modern application infrastructure, 96% of organizations are either using or evaluating Kubernetes. However, as its adoption increases, so do its security risks. Each Kubernetes flavor – whether it's AWS' EKS, Google's GKE, Azure's AKS, or even one of many open source versions – introduces unique vulnerabilities, which, when combined with weaknesses in the underlying infrastructure, can result in severe breaches. Continuous testing is critical to proactively identify and mitigate these risks before attackers can exploit them.

Experience NodeZero's autonomous Kubernetes pentesting firsthand. Discover hidden vulnerabilities in your Kubernetes clusters today.

Explore NodeZero Kubernetes Features:

Visit our website for more information on NodeZero's continuous and autonomous approach to Kubernetes security.

Contact our sales team to arrange a proof of value session and see how NodeZero can protect your Kubernetes infrastructure.

  @Horizon3ai info@horizon3.ai www.horizon3.ai

HORIZON3.ai
~~TRUST~~ BUT VERIFY