What We Do:

The **NodeZero**™ platform empowers your organization to continuously find, fix, and verify your exploitable attack surface. NodeZero helps you reduce your security risk by autonomously finding exploitable weaknesses in your network, giving you detailed guidance about how to prioritize and fix them, and helping you immediately verify that your fixes are effective. There are no required agents to install, no code to write, and no consultants to hire.

Product Differentiators:

Provides Path, Proof, and Impact: NodeZero shows you the actual attack paths in your environment for every weakness it discovers, revealing and detailing each step an attacker could take to penetrate your defenses. It uncovers blind spots in your security posture that go beyond known CVEs and patchable vulnerabilities, such as easily compromised credentials, exposed data, misconfigurations, poor security controls, and weak policies. Weaknesses are prioritized based on their impact on your organization so you know immediately what you should fix first. NodeZero also provides detailed guidance to support your remediation.

Autonomous Operations: The NodeZero platform offers a growing list of operations to help you assess and validate your security posture: internal pentesting, external pentesting, AD password audit, and N-day testing.

Breadth of Coverage: On-prem infrastructure, external attack surface, cloud infrastructure, identity and access management infrastructure, data infrastructure, and more.

Autonomously Chains Attack Vectors: NodeZero pivots through your network, chaining weaknesses together just as an attacker would and then safely exploits them.

Prioritizes: NodeZero shows you what weaknesses are truly exploitable in your network and which have the most critical impacts to your organization so you can prioritize your remediation efforts. It also identifies systemic issues that allow you to remediate many weaknesses with a single change, such as a policy fix.

Requires No Agents or Special Hardware: NodeZero is a true self-service SaaS offering that is safe to run in production. It has no hardware or software for you to maintain, and requires no persistent or credentialed agents.

Continuous, Unlimited, and Orchestrated Deployments:
We don't want to provide a snapshot-in-time; we want to empower your daily security standup, helping you continuously improve your effectiveness. You can schedule and run as many pentests as you want against your largest networks and run multiple pentests at the same time.

Start your free trial now.

https://www.horizon3.ai/trial

In this autonomous pentest attack path, NodeZero exploited two weaknesses — a Java JMX misconfiguration and SAM credential dumping — to achieve domain compromise.

Workflow Examples:

1 **Continuous Vulnerability Detection:** Deploy NodeZero across your infrastructure to continuously monitor and identify vulnerabilities. Upon detection, NodeZero provides immediate notification and detailed reports, prompting your security team to begin remediation immediately. This workflow helps reduce your attack surface and the time-to-remediate.

2 **Efficient Remediation Verification:** After your team applies a fix to address a detected vulnerability, use NodeZero to retest the area and verify the effectiveness of the remediation. This quick verification process can reduce the likelihood of leaving unresolved or insufficiently addressed vulnerabilities.

3 **Prioritization of Vulnerabilities:** Use NodeZero to rank identified vulnerabilities based on severity, exploitability, and potential impact on your business. This can guide your team in prioritizing remediation efforts, ensuring that the most critical vulnerabilities are addressed first.

4 **Compliance Assurance:** Use NodeZero's continuous testing and detailed reporting to demonstrate compliance with various cybersecurity regulations including SOC2, HIPAA, DORA, CMMC, and GDPR. The reports can serve as evidence of your organization's proactive approach to identifying and addressing vulnerabilities.

5 **Proactive Threat Hunting:** Use the data from NodeZero's continuous pentesting to feed into your threat hunting efforts. Analyze patterns in the identified vulnerabilities, look for anomalies, and preemptively hunt for potential threats. This proactive approach can enhance your ability to detect and respond to threats early.

6 **Identifying Data at Risk:** Utilize NodeZero to perform a penetration test, simulating the behavior of an attacker attempting to gain unauthorized access to sensitive data. NodeZero identifies the vulnerabilities that could potentially lead to data exposure. Once vulnerabilities are identified, map them to the data assets they could compromise. This gives you an understanding of which data is at risk.

7 **Determining the Blast Radius of a Compromised Credential:** Use NodeZero to attack with a compromised credential. The scenario should attempt to escalate privileges, gain lateral movement within the network, and access sensitive data. The extent of access achieved in the scenario defines the blast radius of the compromised credential.

8 **Verifying the Effectiveness of Credential Policies:** Use NodeZero to execute a credential-based attack, attempting to compromise and reuse credentials based on your organization's credential policies. The success or failure of these attacks can provide insights into the effectiveness of your credential policies.

9 **Verifying the Effectiveness of Security Tools like EDR and SIEM:** After deploying NodeZero for autonomous pentesting, monitor the alerts and responses from your EDR (Endpoint Detection and Response) and SIEM (Security Information and Event Management) systems. If these tools are detecting and responding to the threats effectively, they are functioning as expected. If not, it might indicate a need for tuning or upgrading these security tools.

Start your free trial now.

https://www.horizon3.ai/trial

