HORIZON3.ai
~~TRUST BUT~~ VERIFY

CAPABILITY STATEMENT

VANDIS

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 that go beyond known CVEs and patchable vulnerabilities, such as easily compromised credentials, exposed data, misconfigurations, poor security controls, and weak policies.

Product Differentiators:

Provides Path, Proof, and Impact: NodeZero shows you the actual attack paths in your environment for every weakness it discovers, showing the proof of where it was able to get past your defenses. Weaknesses are ranked based on their impact on your organization.

Autonomous Operations: NodeZero offers a growing list of operations to help you assess and validate your security posture: internal pentesting, external pentesting, AD password audit, N-day testing, and Phishing Impact 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 maneuvers through your network, chaining weaknesses together just as an attacker would and then safely exploits them.

Prioritizes and Streamlines Remediation: NodeZero shows you what weaknesses are truly exploitable in your network and which have the most critical impacts so you can prioritize your work. It delivers detailed remediation guidance and calls out opportunities to fix systemic issues that can eliminate many weaknesses at once. Use 1-click verify to verify your fixes are effective.

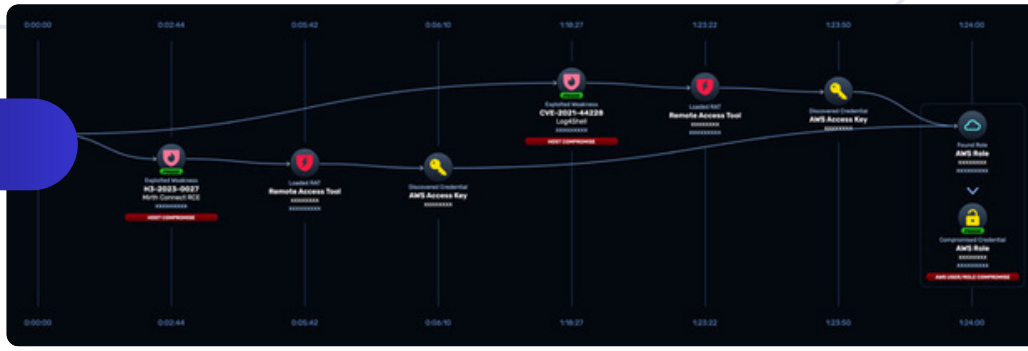
Preemptive Threat Intelligence: Alerts from the Horizon3.ai Attack Team when emerging threats are proven to impact your organization enable you to mobilize your defenses in the NodeZero Rapid Response center.

Continuous, Unlimited, and Orchestrated Deployments: Continuously improve your effectiveness. Include a very broad scope in a single test, orchestrate 100+ concurrent tests, and simultaneously test your enterprise from different attacker perspectives. You can schedule and run as many pentests as you want against your largest networks and run multiple pentests at the same time.

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.

Contact us at info@vandis.com.

REQUEST A DEMO



This attack path shows how NodeZero used a remote access tool to compromise an Amazon Web Services (AWS) credential.

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 1-click verify 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 **Preemptively Respond to Emerging Threats:** Use the NodeZero Rapid Response center to streamline your response to emerging threats. Receive real-time alerts when the Attack Team identifies a nascent threat that impacts your organization. Monitor the status of the vulnerability and learn how to mitigate or remediate as appropriate. Gain access to early exploits to quickly assess your assets and prioritize your activities.

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 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.

Contact us at info@vandis.com.

REQUEST A DEMO

HORIZON3.ai
~~TRUST BUT~~ VERIFY

VANDIS