Sec4good

CAPABILITY STATEMENT

HORIZON3.ai
~~TRUST BUT~~ VERIFY

What We Do:

The **NodeZero**™ platform empowers your organization to continuously find, fix, and verify your exploitable attack surface across your entire digital infrastructure. 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:

Autonomously Chains Attack Vectors: NodeZero maneuvers through your cloud and on-premises environments, chaining weaknesses together just as an attacker would and then safely exploits them.

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.

Breadth of Coverage: NodeZero offers a growing list of operations to help you assess your on-prem infrastructure, external attack surface, cloud infrastructure, identity and access management infrastructure, data infrastructure, blast radius from phished credentials, and more.

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, including fixes for systemic issues that will eliminate many weaknesses. Use 1-click verify to confirm your fixes are effective.

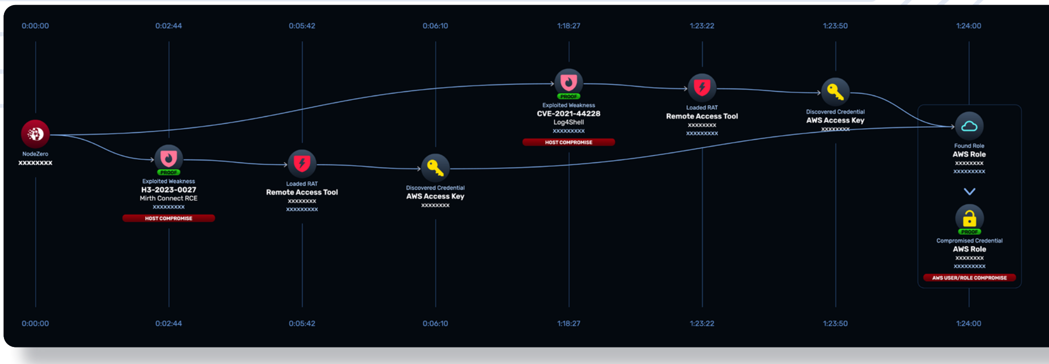
Preemptive Threat Intelligence: Alerts from the Horizon3.ai Attack Team about emerging threats that are proven to impact your organization enable you to mobilize your defenses in the NodeZero Rapid Response center.

Early Threat Detection: NodeZero Tripwires™ enables you to rapidly respond to active threats in high-risk areas of your environment. NodeZero automatically deploys decoys along proven attack paths. You're alerted when malicious activity is detected.

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.

Requires No Agents or Special Hardware: NodeZero is a true self-service SaaS offering that is safe to run in production. No hardware or software to maintain; no persistent or credentialed agents required.

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



Value of NodeZero Platform:

1 **Continuous Vulnerability Detection:** Deploy NodeZero across your infrastructure to continuously monitor and identify exploitable 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 **Early Threat Detection:** Routinely use NodeZero Tripwires™ with your NodeZero pentests. During testing, NodeZero automatically drops appropriate tripwires when it exploits a vulnerability, adding protection before the pentest event is complete. NodeZero alerts you when there are attempts to run tripwire processes or use tripwire credentials.

6 **Validate the Effectiveness of your IAM policies:** Identify cloud-based IAM weaknesses by launching a pentest from a privileged perspective for added visibility. NodeZero will surface vulnerabilities, overexposed or misconfigured public assets, and highlight IAM rules that can be abused for privilege escalation.

7 **Understand a Credential's Blast Radius:** Use the Phishing Impact test to understand the blast radius of phished credentials. NodeZero will attempt to escalate privileges, gain lateral movement within the network, and access sensitive data.

8 **Verify EDR and SIEM Effectiveness:** 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.