HORIZON3.ai

~~TRUST BUT~~ VERIFY

NodeZero Tripwires™

Detect unauthorized access or malicious activity

Every minute that an attacker lurks undetected in your network increases your risk of economic and reputational damage.

NodeZero Tripwires™ leverages autonomous pentesting to enhance your threat detection and response workflow:

- Rapidly respond to indicators of active threats in high-risk areas of your environment
- Automatically deploy deception technology in proven attack paths for maximum effect
- Integrate malicious activity alerts into your existing threat detection and response workflows

Deception Done Differently

NodeZero strategically deploys decoys – such as fake files and fake credentials – along proven attack paths in your environment during autonomous pentests.

Here's how it works:

- You select the Tripwires option for any internal, external, Phishing Impact, or Rapid Response pentest to give NodeZero permission to drop tripwires during the test.
- During the test, NodeZero deploys tripwires only in assets revealed to be exploitable.
- When a tripwire is triggered, you're immediately alerted with relevant information to inform your response.

Key Features

Automated Deployment: Seamlessly integrated with NodeZero's autonomous pentesting, tripwires are automatically deployed in high-risk areas where it matters most.

Real-Time Alerts: When a malicious actor interacts with a tripwire, you'll receive an immediate alert with detailed information about the attempt, the location, and the potential impact.

Low False-Positive Rate: High-quality signal ensures that alerts are meaningful and actionable, minimizing the occurrence of false positives.

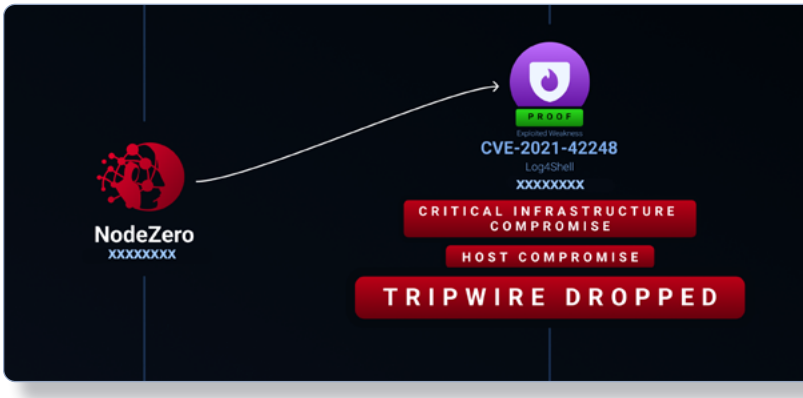
Versatile Tripwire Types: Deploy a variety of tripwires to detect unauthorized access attempts across different attack vectors. Types include AWS API Key, Azure Login Certificate, mysqldump, Windows Suspicious Process Monitor, and Kubeconfig.

Easy-to-Use Management Console: Centralized dashboard for managing all deployed tripwires and viewing alert histories. Simple notification controls.

Integration with Security Tools: Easily integrate Tripwires with existing SIEMs and other security tools into your incident response workflows.

Strategic, Autonomous Tripwires Deployment

NodeZero Tripwires leverages NodeZero's unique ability to use the attacker's perspective to improve your security posture. As NodeZero maneuvers autonomously through your environment, NodeZero Tripwires will automatically deploy tripwires in assets that are likely to be attacked.



Workflow Examples

Detect Credential Compromise

Use Tripwires to detect credential compromise across your entire digital infrastructure. Example: After gaining domain admin access, NodeZero pivoted to Azure Entra ID and compromised the account of the Azure global admin. During the test, NodeZero strategically placed Windows Suspicious Process Monitor and Azure Login Certificate tripwires on the domain admin, the Azure Entra ID global admin's machines, and other key hosts containing sensitive data. NodeZero alerts the team when a threat actor attempts to use the Azure credential tripwire or run a tripwired process.

Augment Your Phishing Simulations

Expand the benefit of the Phishing Impact test by using Tripwires to detect whether phishing-prone credentials have been compromised. Example: During a Phishing Impact test, NodeZero harvests phishing-prone credentials with admin privileges. It uses the credentials to deploy tripwires to a network share, dropping Azure login keys across multiple user directories to detect and alert you to malicious activity.

Detect Threat Activity on Emerging Threats

Protect your organization in the time critical window between the identification of an emerging threat and the availability of a security update. Example: During a Rapid Response pentest, NodeZero identifies a host that can be compromised with the new vulnerability. NodeZero immediately alerts you that your organization is impacted by this threat and simultaneously deploys a tripwire to the location. Even before the pentest is complete, your team is alerted when a threat actor attempts to run a process indicative of malicious intent. The early warning delivered with relevant details allows you to escalate the appropriate response in that critical early time window that attackers are primed to exploit.

If you are interested in participating in our Tripwires Early Adopter Program, contact h3earlyadopter@horizon3.ai.