HORIZON3.ai
~~TRUST BUT~~ VERIFY

CAPABILITY STATEMENT

Core Competencies: We deliver autonomous penetration testing as a service, enabling you to run self-service pentests to find, fix, and verify the resolution of security weaknesses before attackers can exploit them. There are no agents to install, no code to write, and no consultants to hire.

Company Data

Our story: We are a fusion of former U.S. Special Ops cyber operators, startup engineers, and frustrated cybersecurity practitioners. We see the world for what it is – bloated security tools, alert fatigue, reports filled with false positives, "checkbox" security culture, and consultants trying to pitch their "expertise."

Our thesis: Use the "Attacker's Perspective" to cut through the noise and help you find and fix exploitable attack vectors. We deliver this by running continuous, autonomous pentest and red team operations, building "cyber terrain maps," and generating analytics to identify angles of attack.

Our vision: Be the most trusted autonomous pentesting platform in the industry. We're not just a pentesting company; we're a data company that will use our cyber terrain maps to deliver disruptive security products. Legacy pentesting and red team operations are the first pillars to fall.

Product Differentiators

Agentless: NodeZero is a true self-service SaaS offering that is safe to run in production and requires no persistent or credentialed agents.

Path, Proof, and Impact: NodeZero provides visibility to see what's most vulnerable and create bias for immediate action – Find, Fix, and Verify exploitable threats.

Autonomously chained attack vectors: Our graph-based platform enables us to take one problem and combine it with another to achieve a greater impact.

Context Scoring: We focus on the truly exploitable attack paths and report the most critical impacts upfront so customers can prioritize their efforts.

Unlimited deployments: We don't want to provide a snapshot-in-time; we want to power your daily security standup, helping you prove your effectiveness over time.

Strategic Impact

Manufacturing: NodeZero identified COVID-19 temperature scanner kiosks deployed at physical sites with an Android Debugger Bridge port open, allowing access to the system with root privileges.

Media: NodeZero autonomously assessed 3,644 IPs in <3 days, discovering 25 weaknesses (3 critical) across 52 attack vectors leading to three critical impacts, including 332 credentials (including default creds) that led to 45 data resources and 1M+ sensitive files accessible.

IT Services: NodeZero was able to get in and use Secure Shell (SSH) "root" with a 5-character default password and compromise the host.

Entertainment: NodeZero was able to compromise a local host; the SSH service was brute-forced by credential "root" with a default password.

Manufacturing: NodeZero executed a worthy external recon; after more digging, it exposed massive development flaws that were publicly available and exposed their business and brand to risk. No pentest or vulnerability assessment had shown this before.

Financial Services: NodeZero elevated privileges from unauthenticated user to Domain Admin in 7 mins and 19 seconds, identifying significant blindspots in the SOC.

Healthcare: NodeZero identified and proved ZeroLogon (CVE:10) was exploitable despite contrary reporting from Qualys and Microsoft, and uncovered significant errors in their patching process.

Design Principles

Ease of Use: You're up and running an autonomous penetration test in minutes using our self-service portal or API.

Accuracy: Fix problems that can actually be exploited; save you and your team from chasing down unexploitable vulnerabilities and false positives.

Speed: Assess your entire organization in a matter of hours, versus waiting weeks or months for consultants to manually run scans and produce reports.

Coverage: Assess your entire network from the attacker's point of view, not just a sample.

Remediation: Quickly find, fix, and verify that an exploitable problem is no longer a threat.

Benign: Define the scope of the operation – IP ranges it should stay within, IP ranges it should avoid – or let it intelligently identify the scope for you.

Flexibility: You'll have the ability to enable or disable specific attacks, if you want to be extra cautious.