HORIZON3.ai

~~TRUST BUT~~ VERIFY

Horizon3.ai Strengthens Partnerships with Consulting PLUS Program

NodeZero Consulting PLUS Program is the force multiplier to help your clients find and fix attack vectors before criminals exploit them.

Cybersecurity consultants and service providers offer a variety of information technology (IT) services to other businesses. Given their nature, cybersecurity consultants are in a position to deliver immediate impact to their clients.

In a world of ever-evolving cyber threats, our alliance partners must ensure they are providing tier-one cybersecurity services while remaining affordable. The Horizon3.ai NodeZero Consulting PLUS Program helps cybersecurity consultants and service providers better support their clients by offering a service that quickly identifies vulnerabilities, provides fixes, and verifies mitigation.

NodeZero is Horizon3.ai's Autonomous Penetration Testing as a Service (APTaaS) that helps mid-market and enterprise organizations needing to harden their security systems but lacking the internal resources to manage. It is like having a highly skilled, experienced Red Team on-site exploiting the network and then providing all the fixes required.

This license hands skilled cyber consultants a powerful force multiplier to enhance their current service deliverables to grow their business.

The benefits of the NodeZero Consulting PLUS Program include:

- **Unlimited use** of NodeZero for penetration tests.
- **Unlimited sequential penetration test operations.**
- **Unlimited IP Addresses per penetration test operation.**
- **Special pricing for authorized Horizon3.ai Alliance Partners.**
- Ensures a **comprehensive assessment** of a client's security posture and rapid time-to-value.
- Consulting Partner have **access to the Horizon3.ai Customer Success Team** for questions regarding operations reports and any issues that need to be resolved.

Continuous, Autonomous Pentesting with NodeZero

Continuously...

- **Identify** new exploitable attack vectors.
- **Auto** open/track/close tickets with proof.
- **Prioritize** remediations based on impact & effort.
- **Verify** problems have been fixed.
- **Validate** security controls are effective.
- **Benchmark** posture against best practices.
- **Report** posture to board & regulators.

> Averaging **$570K per ransomware payment in 2021**, NodeZero's ability to intelligently verify an attacker's blast radius -- including accessible sensitive data -- is an invauable continuous attestation to a Board when they ask the question:
>
> **"Are we prepared?"**

Not every business can afford a complete cybersecurity team, those businesses trust their cybersecurity consultants to provide them the resources they need to keep their networks secure.

Attackers know the latest vulnerabilities, misconfigurations, and system defaults worth pursuing. They know how to harvest credentials and reuse them all over your network and outside of your network. Attackers know how to chain attack methods together to compromise what is most valuable to your organization.

Thankfully NodeZero is on your side, knows all the attacks better, deploys at the speed of autonomy, and even provides all the fixes to better support your clients. NodeZero does not require additional personnel or equipment and it is very affordable, making it the best all-around APTaaS option on the market today.

Why NodeZero?

Security Impacts Aligned to Business Outcomes

- **Cost reduction** – drastically decrease OpEx for consulting and third-party pentests while reducing CapEx tool spend on duplicative and unused high investment security tools.
- **Cost avoidance** – eliminate the need for siloed and niche tools and costly consultants which inevitably incur additional maintenance footprint and training debt on your annual budget.
- **Risk reduction** – remove risk decisions with unlimited access to NodeZero, which continuously assesses and proves reachability to sensitive data and backups; reduce quantifiable risk inherent in persistent tools using an agentless, unauthenticated, and ephemeral approach.
- **Increase capacity** – empower security practitioners to fix what matters faster with safe and accurate automation.

HORIZON3.ai
~~TRUST BUT~~ VERIFY