HORIZON3.ai

~~TRUST BUT~~ VERIFY

Autonomous Penetration Testing with Horizon3.ai

The NodeZero™ platform is easy-to-use, safe for production, and scales to support your largest networks. You are empowered to test a very broad scope in a single test, orchestrate tests concurrently, and simultaneously test your enterprise from different attacker perspectives.

An autonomous penetration test with NodeZero brings value to your organization by identifying attack vectors and providing proof of exploitability. It can provide evidence that defensive controls are implemented effectively and focus remediation efforts on your organization's most critical weaknesses.

Two key types of penetration tests are: external penetration tests to ensure you have a strong perimeter; and internal penetration tests to discover weaknesses that could be exploited by an attacker who gains a foothold.

Continuously Verify Your Security Posture.

Are you secure? How do you know? Don't wait for a breach to find out. Continuously test your security posture to ensure no exploitable vulnerability, misconfiguration, or harvested credential could leave you vulnerable. External pentests evaluate your external facing assets to identify how an adversary may be able to identify and exploit weaknesses to enter your network.

NodeZero external penetration tests identify attack vectors that include:

- Vulnerabilities and misconfigurations that go beyond Common Vulnerabilities and Exposures (CVEs) that attackers can exploit to breach your network perimeter
- Compromised credentials that attackers can abuse to gain unauthorized access to your organization's assets and data
- Sensitive data out in the open that attackers can discover
- Shadow IT projects and end-of-life assets that expand your attack surface

Presume Breach to Limit Damage.

In today's environment of constant social engineering attacks via email, availability of stolen credentials, and misconfigured systems, organizations must presume an initial breach has already occurred and attackers have a foothold in their internal systems.

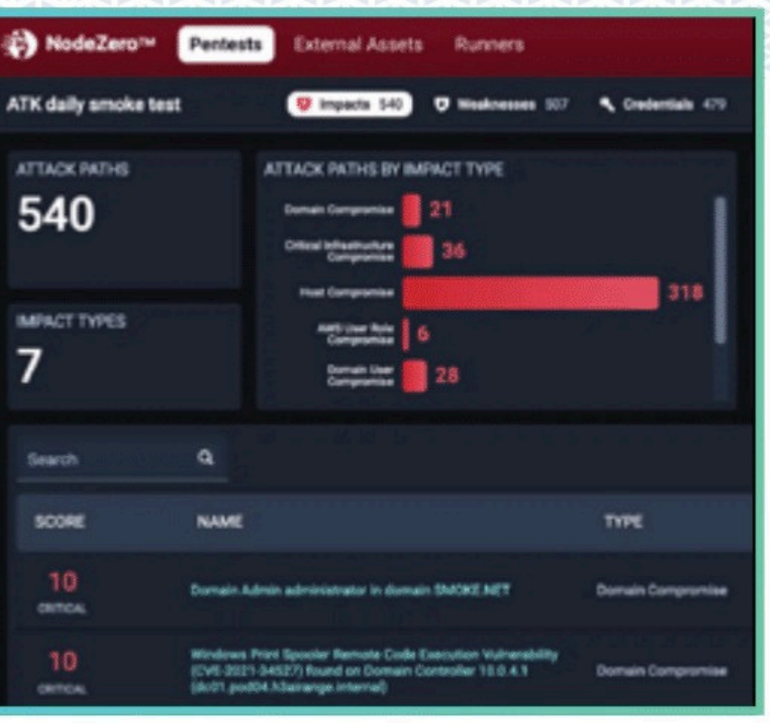
A NodeZero internal penetration test starts with the acceptance that an attacker can gain access to your internal network where your sensitive data resides. From that starting point, internal pentests determine what a malicious actor can access and accomplish:

- **Can they access additional credentials and privileges?**
- **What weaknesses, misconfigurations, and vulnerabilities can they exploit to move laterally?**
- **What sensitive data can they access?**
- **Which exact issues must be remediated – and how – to prevent a successful attack?**

Not a Vulnerability Scanner

Vulnerability scanners search your perimeter and internal systems for unpatched applications and run rules to look for specific known vulnerabilities as detailed by the National Institute of Standards and Technology (NIST) CVE. Scanners provide reports on those systems they 'think' are unpatched and those CVEs they can identify. The noise from low criticality issues can result in teams spending cycles on non-exploitable issues instead of focusing their efforts on the weaknesses that have the greatest impact on their organization.

Importantly, vulnerability scanners do not identify systems that were incorrectly patched, or identify exploitable attack paths that may be available to adversaries who chain together weaknesses in their attacks.



Vulnerable ≠ Exploitable

In contrast, NodeZero identifies weaknesses across your external, on-prem, and cloud systems, as well as your users, even when vulnerability scanners and patch management systems show that security updates have been successful. It provides step-by-step path and proof of each successful exploitation so your team understands how and where an attacker can execute and attack. The platform prioritizes the weaknesses and their impacts for your organization so that your team can focus on fixing what matters most instead of wasting cycles on non-exploitable issues.

NodeZero

Continuously secure your security posture.
NodeZero solves the problem of expensive manual penetration testing and goes beyond the limitations of other automated solutions.
NodeZero is an *autonomous* penetration testing solution – a "self-service" offering that is safe to run in production and requires no persistent or credentialed agents.
It assesses systems with the flexibility and contextual decision making that manual pentesters use, but faster, more completely, and with more actionable results.

~~Manual~~
~~Crowdsourced~~
~~Automated~~
Autonomous Pentesting

HORIZON3.ai
~~TRUST BUT~~ VERIFY

What is Autonomous Penetration Testing?

NodeZero is different from other pentesting solutions – combining the lower cost and high frequency testing capabilities of automated pentesting with the expertise, thoroughness, and precision of manual pentests performed by highly skilled security professionals.
The result is an ability to run continuous purple teaming exercises at a low annual cost.
Pentesting has evolved from manual, to crowdsourced, to automated, and now autonomous.

Manual pentesting requires a trained security resource using commercial and specialized tools to explore an application or system and identify weaknesses. The effectiveness (and cost) of a manual pentest is dependent on the time allotted to the test and the skill of the pentester, leading many organizations to save costs by providing credentials to pentesters. Start to finish, manual pentests often take months to complete and only address a small fraction of an organization's attack surface. Remediation guidance for issues found may be very limited. Further, the high cost of manual pentests prevents organizations from using them frequently, such as after a system is patched to ensure the update was completed correctly.

Automated pentesting is a simple "point and click" approach using commercial dynamic analysis tools. The tool is provided a URL or IP address and spiders the application to identify fields where a malicious user could input data. The tool then "fuzzes" data to the fields to attempt to prove the presence of input validation weaknesses that could be exploited by a skilled attacker or overwhelm the application in a denial of service attack. These tests normally run in a day or two. A drawback is that some automated pentests generate a lot of noise by identifying unproven results that defenders must research to determine if they require remediation.

Crowdsourced pentesting includes manual pentests, but relies on a network of independent security researchers who are paid "per vulnerability identified" (plus a platform fee to the vendor). Crowdsourced pentests have the advantage of being open ended, meaning – in theory – you can have people searching for issues every day for months. They can be quite expensive if there are large numbers of vulnerabilities, and findings often lack proof of exploitability (e.g., unpatched systems, open ports, etc.) leading development teams to spend time on non-critical issues.

Autonomous pentesting combines the benefits of automated pentesting; more frequent testing, lower costs, and no requirements for internal security expertise, with those of manual pentests: deeper testing, contextual decision making, and proven exploitability. Autonomous pentesting does not require credentials to start. It can chain together weaknesses like a skilled adversary and automatically generate attack paths to isolate the root cause of an exploit. This allows defenders to understand precisely what changes are needed to protect an application.

HORIZON3.ai
~~TRUST BUT~~ VERIFY

How NodeZero Works

Reconnaissance

Any successful attack requires intelligence on the target. NodeZero starts with unauthenticated access to the system, then identifies all hosts, misconfigurations, open port, and searches for credentials.

Maneuver Loop

NodeZero orchestrates over 100 offensive tools to discover and exploit weaknesses in your network just as an attacker would. It moves laterally in your environment by:

- Compromising credentials through credential attacks
- Mining exposed data
- Bypassing security controls
- Exploiting key vulnerabilities and misconfigurations

Verified Attack Plans

To simplify prioritization and remediation, results are provided as "Proofs" with graphical and textual representations of each step in a successful attack. This includes which tactics were used, which weaknesses were identified and exploited, how credentials were obtained, and the paths taken to gain privileges and access to systems.

Impact

NodeZero identifies and reports on data at risk across physical and virtual environments such as misconfigured file shares, insecure data transfer protocols, or weak access controls. It identifies data exposure including payment card information, social security card numbers, and other personally identifiable information (PII) that increases your risk of ransomware and can jeopardize your overall security and regulatory compliance.

Contextual Scoring

NodeZero evaluates and prioritizes each weakness by its role in the successful attack in your environment – not by the generic base Common Vulnerability Scoring System (CVSS) score. You can quickly identify those weaknesses that present the greatest threat to your organization and must be addressed immediately, and which can be safely deferred.

Actionable Remediation

NodeZero provides precise and actionable remediation guidance, allowing security and operations to resolve issues at the root cause quickly.

Meaningful Reporting

NodeZero delivers a rich – and always growing – set of reports for you to use throughout your workflow, including the Executive Summary and Fix Actions report. The reports are easily customized and co-branded.

Ready to Learn More?

NodeZero helps you continuously improve your security effectiveness with ongoing, unlimited autonomous pentests and other key security operations. It is safe to run in production and requires no persistent or credentialed agents. **Find and fix attack vectors before attackers can exploit them**.

- **Sign up for your free trial today.**

https://witzcybersecurity.com/contact/

Witz CYBERSECURITY
Australian & New Zealand partner

HORIZON3.ai
~~TRUST~~ BUT VERIFY