HORIZON3.ai

~~TRUST BUT~~ VERIFY

CASE STUDY

Vulnerable ≠ Exploitable

A lesson on prioritization

@Horizon3ai ✉ info@horizon3.ai www.horizon3.ai

The Typical Approach

Pen testers, vulnerability scanners, and installed agents alert on potential vulnerabilities and breaches. You receive a list, or a notification, and you respond. **Ever wonder how much of your time and effort is being wasted fixing things that don't actually matter?**

You may be surprised to hear that a large majority of all vulnerabilities are unexploitable. According to data compiled by Kenna, in 2020, only 2.7% of the vulnerabilities found appeared to be exploitable and only 0.4% of those vulnerabilities were actually observed to be exploited at all.[1]

The prioritization of these low-risk or no-risk vulnerabilities alongside, or even above, the truly exploitable vulnerabilities can actually cause an organization's security posture to suffer. It takes significant time and coordination to find the asset owners, bring them up to speed on the issue, prepare downtime for the asset, remediate the issue, and then confirm that the issue is remediated. Meanwhile, more critical vulnerabilities are waiting in line for their turn to be remediated. **If you can't properly prioritize, you will never secure your network.**

A client came to Horizon3.ai with the goal of validating the services they were using for pentesting, vulnerability scanning and remediation. Their IT services had all been outsourced to a managed security service provider (MSSP) with a hefty price tag; they wanted to make sure they were getting what they paid for.

The MSSP had just conducted their annual pentest of the organization's network environment. Horizon3.ai used NodeZero to assess the organization's network, with the following comparative results:

Horizon3.ai NodeZero	VS	MSSP Manual Pentest
Assessed **3,644 hosts**	COVERAGE	Assessed only ~600 hosts
Full coverage in **2.75 days**	SPEED	Partial coverage took over 1 week
Minutes to run operation, immediate results	EFFORT	Weeks to prepare, weeks for results
• Critical/High exploitable findings discovered on many more hosts (BlueKeep, Eternal Blue, etc.) • Several additional critical/high exploitable findings found (IPMI, GhostCat, Cisco Smart Install, etc.) • Surfaced contents of several large SMB/NFS shares	ACCURACY	• Nearly 80% (22 of 28) of critical findings are either **not exploitable, or are extremely impractical to exploit** • Several critical/high vulnerabilities not detected (IPMI, guessable root access to databases, credentials/keys stored in an open share… **all of which NodeZero found**)

[1] https://www.kennaresearch.com/a-decade-of-insights/

Why Coverage and Accuracy matter

The hardest part of cyber security is **deciding what NOT to fix** because of limited time and resources.

Manual Pen Testing creates an incomplete snapshot:

- No exploits exist, or conditions to exploit are extremely unlikely, for 22/28 of the MSSP's critical findings
- Poor enumeration leads to blind spots and incomplete fingerprinting - port scans are not enough!
- Partial coverage leads to missed critical findings

Horizon3.ai NodeZero	VS	**MSSP Manual Pentest**
Automatically identified 4 of 5 exploitable issues found by the MSSP VMWare issue appears to be a false positive or was remediated between ops	**VALID CRITICAL FINDINGS**	5 of 28 issues marked critical are exploitable 1 of 28 (VMware) may be a false positive
Found on **12 hosts**	**BLUEKEEP** (LEADS TO RCE)	Found on 1 host
Found on **14 hosts**	**ETERNALBLUE** (LEADS TO RCE)	Found on 2 hosts
Found **14 file shares**, over **2 million files** surfaced, likely containing sensitive data (**multiple SSH/AWS keys found**)	**'GUEST' ACCESS TO CIFS SHARES**	Found 4 file shares
Achieved **root-access to 3 database servers,** pilfered hashes from **9 hosts with vulnerable IPMI** configurations	**ADDITIONAL CRITICAL/HIGH WEAKNESSESS**	NONE

Fixing 79% of the critical issues highlighted in the MSSP's report would have been an inefficient use of time and effort. These so-called "critical issues" did not have exploits, were blindly assumed due to poor enumeration, or the conditions for exploitability were extremely unlikely.

Meanwhile, the MSSP's team only identified one host vulnerable to BlueKeep, while NodeZero found an additional 11. NodeZero also proved three additional critical/high weaknesses, including easily guessable root access to a database server.

When the noise is removed, the critical findings are revealed.

The Horizon3.ai Difference

Thinking like an attacker gives you a distinct advantage as you devise a defensive strategy.

The attacker's perspective asks:

- What is an attacker interested in doing or achieving?
- What methods are realistically at their disposal?
- What things about your environment makes achieving their intentions possible, or even easy?

We believe that these questions can only be answered by an "attacker-mindset" pentest, which should be performed frequently on your entire environment so risks do not accrue, and should produce findings that guide your remediation actions with a heavy bias towards efficiency and return on investment.

Horizon3.ai delivers these outcomes through NodeZero, our autonomous penetration testing-as-a-service (APTaaS) platform. NodeZero is an on-demand, self-service platform that is safe to run in production and requires no persistent or credentialed agents.

Within our Portal, we provide the following supporting information for every weakness NodeZero finds:

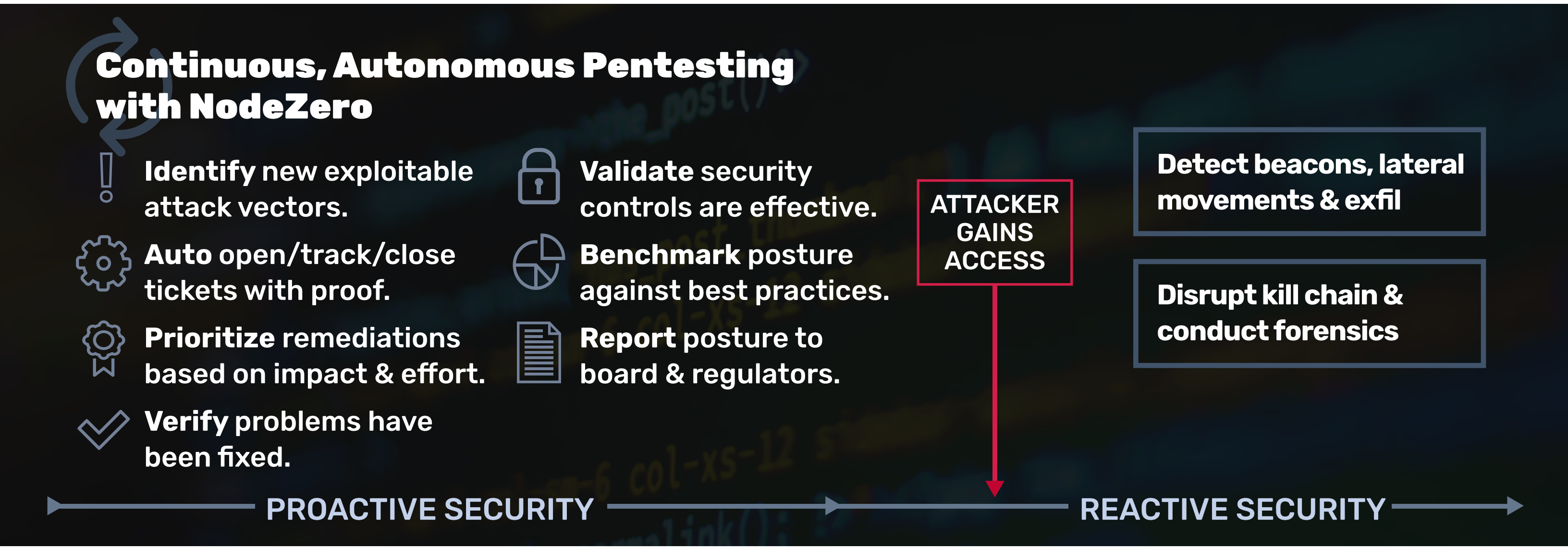
- Path NodeZero followed to identify/discover the weakness.
- Proof of exploitability of the weakness.
- Context and severity of the finding, which can be used to determine business impact.
- Fix action report you can follow to remediate the weaknesses.

> For me, **the biggest benefit is the attack path identification and actual prioritization of the vulnerabilites**. Other tools simply pull the CVE value, and we get hundreds of criticals and highs.

The Future State

Overall, the comparison between the MSSP's report and the NodeZero report shows that NodeZero provides broader coverage, proves exploitability, contextualizes weaknesses, and provides the defensive team with the information they need to fix what matters.

Our work with this client exemplifies the need for a proactive security posture that includes continuous assessment, so you can **catch up**, **keep up** and even **stay ahead**.



Continuous, Autonomous Pentesting with NodeZero

- **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.

ATTACKER GAINS ACCESS

Detect beacons, lateral movements & exfil

Disrupt kill chain & conduct forensics

PROACTIVE SECURITY

REACTIVE SECURITY

Catch Up

Identify exploitable attack paths that must be fixed immediately, significantly reducing the opportunities for exploitation, sensitive data exposure, elevated privileges or remote code execution.

Your first NodeZero operation will provide this insight and minimize the time spent dealing with false positives.

Keep Up

Establish a purple team culture to **find** exploitable problems, **fix** them and then **verify** that the problems no longer exist. Your red team should be working with your blue team to maximize coordination.

You can run multiple NodeZero operations per week – our licenses give you unlimited access.

Use NodeZero's compare feature to power your security standups.

Stay Ahead

Continuously verify your security controls – tools, processes, policies – by measuring and optimizing your detection, remediation and compliance response times.

Use our reports to show your leadership and board where you stand. Not just a compliance checkbox; this is effective security.

HORIZON3.ai

~~TRUST BUT~~ VERIFY

About Horizon3.ai

Horizon3.ai's mission is to help you find and fix attack vectors before attackers can exploit them. NodeZero, our autonomous penetration testing solution, is an unlimited, self-service SaaS offering that is safe to run in production, available on-demand, and requires no persistent or credentialed agents. See your enterprise through the eyes of the attacker, identify your ineffective security controls, and ensure your limited time and resources are spent fixing problems that matter. Not just a compliance checkbox; this is effective security. Founded in 2019 by industry, US Special Operations, and US National Security veterans, Horizon3.ai is headquartered in San Francisco, CA.

www.horizon3.ai

Ready to Learn More?

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

https://www.horizon3.ai/demo