HORIZON3.ai

~~TRUST BUT~~ VERIFY

2023 YEAR IN REVIEW

Proactive Cybersecurity **Unleashed**

Observations of the Challenges Organizations Continue to Face

Table of Contents

HORIZON3.ai
~~TRUST BUT~~ VERIFY

Letter from the Authors

Welcome to the second annual Year in Review for 2023! We are excited to share how Horizon3.ai's customers are taking a proactive approach to cybersecurity by conducting autonomous pentests with the NodeZero™ platform.

In 2022, we introduced the **Through the Eyes of the Attacker** perspective by revamping NodeZero to offer fresh and powerful features. Through this upgrade, NodeZero enhances how users **attack** their environments and enables them to take back their environments by proactively protecting against attacks. Additionally, Horizon3.ai still enables customers to ask:

- What does my environment look like?
- Are my security tools effective?
- Did we detect the right actions?
- Are we logging the right things?
- Is my sensitive data, or are my crown jewels and keys to the kingdom safe?

Horizon3.ai emphasizes the importance of a proactive approach in obtaining honest, accurate, and relevant answers to these critical questions. To achieve this, we advocate for adopting the perspective of an attacker and consistently attacking your respective environments using NodeZero, just as a nefarious cyber threat actor would do. This proactive stance empowers us and our customers to identify exploitable vulnerabilities quickly, address the most critical issues, and subsequently validate the effectiveness of these corrective actions though the **Find, Fix, Verify loop.**

In pursuit of this strategy, we are eager to share a fresh perspective with you, illustrating how our diverse range of customers across various industries and sectors utilize NodeZero. They employ this platform to proactively discover, rectify, and verify exploitable misconfigurations and vulnerabilities within their environments, employing real-world tactics, techniques, and procedures (TTPs) commonly used by attackers. Moreover, we will provide insights into the implications of the vulnerabilities and weaknesses identified and offer policy recommendations aimed at enhancing our customers' security posture.

Thank you to the remarkable customers and partners who collaborate with us and help Horizon3.ai enhance our capabilities and products. We trust that this report will be both insightful and instrumental in your pursuit of a stronger security posture while staying ahead of attackers.

- The Horizon3.ai Customer Threat Analytics Team

HORIZON3.ai
~~TRUST BUT~~ VERIFY

INTRODUCTION

NodeZero Continues to Change the Game

NodeZero revolutionizes the landscape for organizations seeking an autonomous pentesting solution, creating a proactive and preemptive strategy that illuminates how an attacker sees your environment and reinforces resilience against cyber threats. Over the past year, NodeZero has redefined pentesting, changing the game for our customers by enabling them to regularly stay ahead of threats and harden their entire environment. Since our last Year in Review, we have seen a sharp increase in daily, monthly, and annual pentests. In 2023, our customers ran a total of nearly 30K pentests, testing 2.05M assets, with 110K of those assets being related to critical impacts, comprised of 450K impact paths and 1.5M discovered weaknesses!

Why do our customers run so many tests? Unlike traditional (manual) pentests, NodeZero allows our customers to run continuous pentests for no additional costs (as shown by Figure 1). NodeZero also allows customers to see a prioritized list of vulnerabilities, proof of exploitation (when available), and highlights of notable events to enable customers to fix what matters first, and to verify those fixes. Additionally, it provides detailed attack paths that allow customers to walk through how an attack could be carried out Through the Eyes of an Attacker, while also showing which vulnerabilities led to specific downstream impacts and what to fix to mitigate other issues throughout the environment. This gives our customers a full graphical representation of actual attack paths that an attacker could use to chain together misconfigurations, vulnerabilities, and weaknesses to compromise their organization.

Figure 1: Transform your organization and adapt to 21st century cyber threats by switching from slow, manual, once-per-year pentesting to continuous, autonomous cybersecurity with NodeZero.

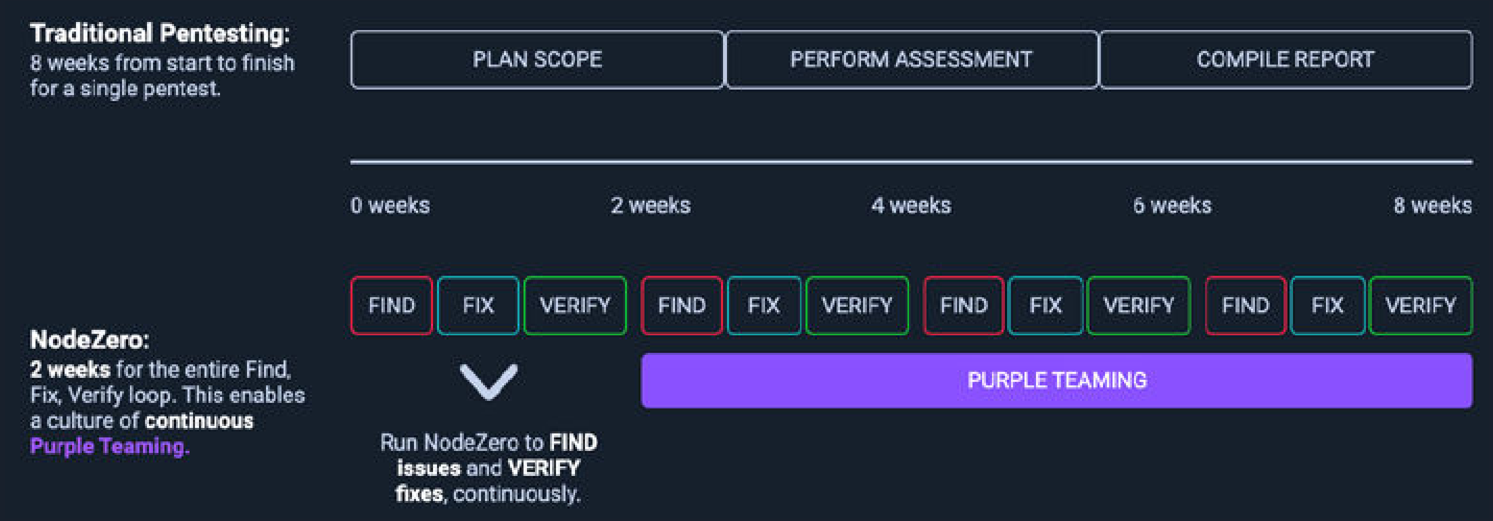
NodeZero vs Traditional Pentesting

	TRADITIONAL PENTESTING	NodeZero
Cost of Coverage A single traditional pentest covering 300 hosts would cost $25,000 on average. With NodeZero you get unlimited pentests for a year at $50/host.	$25,000 per pentest*	$15,000 per year* (unlimited pentests)
Speed A single traditional pentest covering 300 hosts could take up to 8 weeks or more for procurement, planning, execution, and reporting. With NodeZero you get results within hours.	8+ weeks	hours
Fix Action Reports NodeZero provides detailed fix action reports with every pentest.	✗	✓
Continuous Validation: Find, Fix, Verify Your NodeZero license provides for unlimited pentesting that you can deploy year round to verify remediation efforts and identify new exposures in your environment soon after they are introduced.	✗	✓
Mean-Time-to-Remediation (MTTR) Given NodeZero's coverage, speed, detailed fix actions, and continuous validation, your MTTR can be reduced from months to days, if not hours.	1+ months	days
Customer Success Your NodeZero license provides dedicated Customer Success representatives who work with you to optimize the value you get from NodeZero.	✗	✓

** These numbers are based off an environment with 300 hosts.*

HORIZON3.ai
~~TRUST BUT~~ VERIFY

Find. Fix. Verify with NodeZero



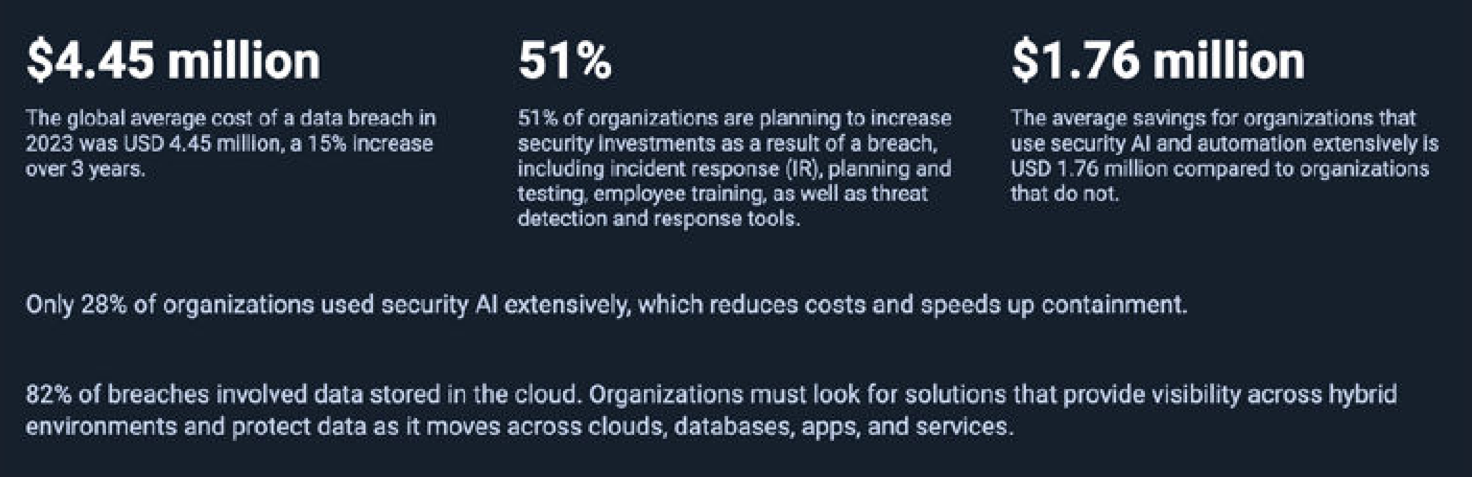
Traditional Pentesting: 8 weeks from start to finish for a single pentest.

NodeZero: **2 weeks** for the entire Find, Fix, Verify loop. This enables a culture of **continuous** **Purple Teaming.**

Run NodeZero to **FIND issues** and **VERIFY fixes**, continuously.

Figure 2: Save time, save money, and increase your cybersecurity resilience by employing NodeZero's Find. Fix. Verify. loop to dramatically reduce the time spent finding, fixing, and verifying security exposures.

Cost of Breach



$4.45 million

The global average cost of a data breach in 2023 was USD 4.45 million, a 15% increase over 3 years.

51%

51% of organizations are planning to increase security investments as a result of a breach, including incident response (IR), planning and testing, employee training, as well as threat detection and response tools.

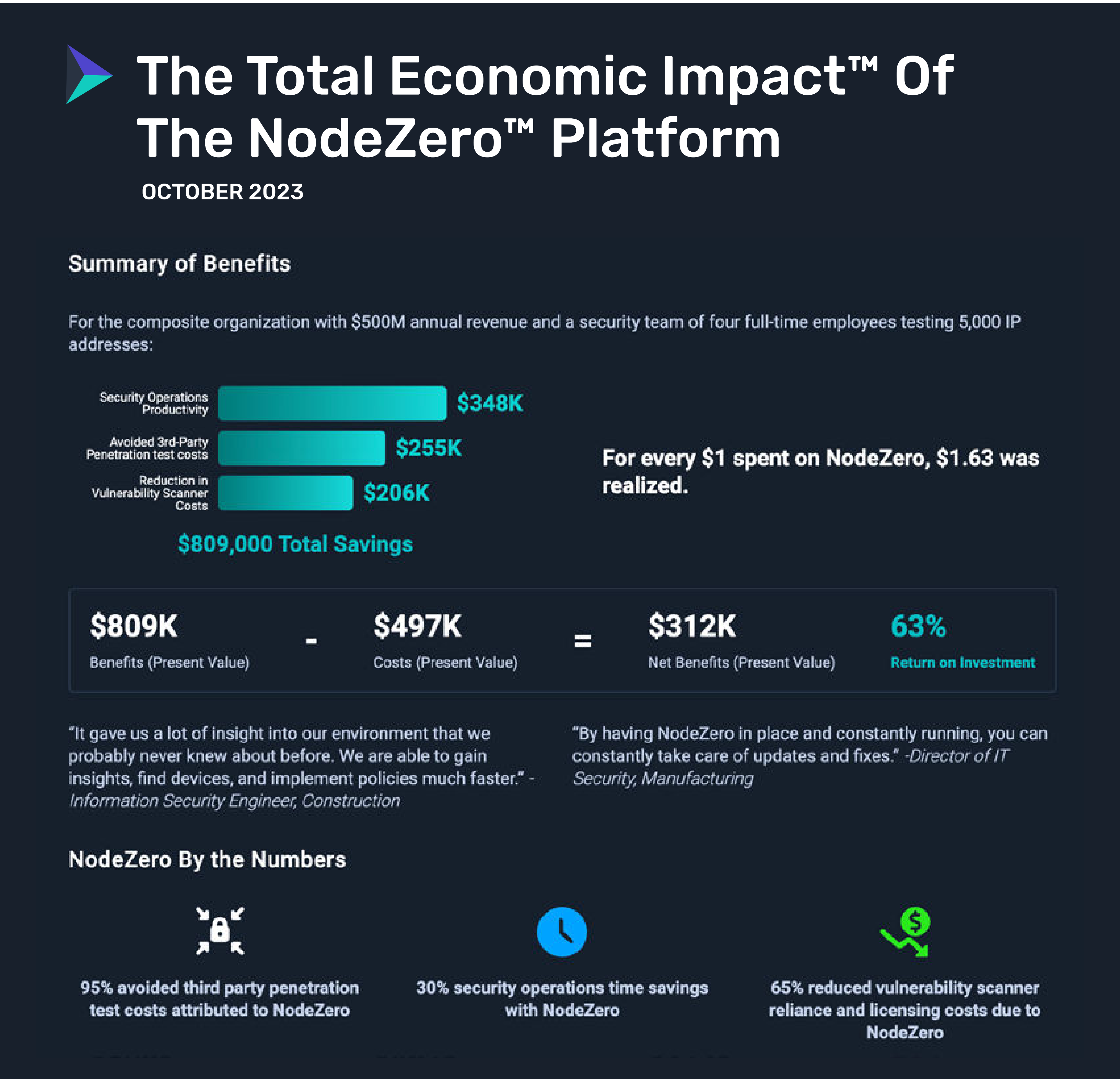
$1.76 million

The average savings for organizations that use security AI and automation extensively is USD 1.76 million compared to organizations that do not.

Only 28% of organizations used security AI extensively, which reduces costs and speeds up containment.

82% of breaches involved data stored in the cloud. Organizations must look for solutions that provide visibility across hybrid environments and protect data as it moves across clouds, databases, apps, and services.

Figure 3: Investing now can save millions... Source: IBM Cost of Breach Report



The Total Economic Impact™ Of The NodeZero™ Platform

OCTOBER 2023

Summary of Benefits

For the composite organization with $500M annual revenue and a security team of four full-time employees testing 5,000 IP addresses:

Security Operations Productivity	$348K
Avoided 3rd-Party Penetration test costs	$255K
Reduction in Vulnerability Scanner Costs	$206K

$809,000 Total Savings

For every $1 spent on NodeZero, $1.63 was realized.

$809K Benefits (Present Value)	-	$497K Costs (Present Value)	=	$312K Net Benefits (Present Value)		63% Return on Investment

"It gave us a lot of insight into our environment that we probably never knew about before. We are able to gain insights, find devices, and implement policies much faster." - *Information Security Engineer, Construction*

"By having NodeZero in place and constantly running, you can constantly take care of updates and fixes." *-Director of IT Security, Manufacturing*

NodeZero By the Numbers

95% avoided third party penetration test costs attributed to NodeZero

30% security operations time savings with NodeZero

65% reduced vulnerability scanner reliance and licensing costs due to NodeZero

Source: "The Total Economic Impact (TM) of the NodeZero(TM) Platform, October 2023," a study Horizon3.ai commissioned from Forrester Consulting.

Figure 4: The Total Economic Impact™ Of The NodeZero™ Platform: Forrester Consulting interviewed six representatives at four organizations using the Horizon3.ai NodeZero platform to evaluate the three-year financial impact of using NodeZero.

Here are some additional reasons why customers implement NodeZero to help proactively Find, Fix, and Verify vulnerabilities before they are exploited, while ensuring they stay compliant with industry standards and maintain uninterrupted business operations:

- **Continuous Security Assessments:** Traditional penetration tests are often conducted annually, leaving organizations vulnerable between tests. With NodeZero, security assessments can be performed more frequently, providing real-time insights into vulnerabilities and potential threats.
- **Efficiency, Speed, and Scalability:** NodeZero can handle the increased scope and complexity of modern IT environments, ensuring thorough assessments without compromising on speed or accuracy. It can scan and analyze large and complex networks or systems much faster than manual testing. This efficiency enables organizations to identify and address vulnerabilities quickly, reducing the window of exposure to potential cyber threats. Further, as businesses expand and technology infrastructures grow more intricate, the scalability of autonomous penetration testing becomes crucial.
- **Adaptability to Evolving Threats:** The cybersecurity landscape is dynamic and constantly changing, with new threats emerging daily. NodeZero enables customers to proactively illuminate new threats and improve their ability to detect and assess vulnerabilities effectively.
- **Risk Prioritization:** NodeZero doesn't just tell our customers what it found; it prioritizes vulnerabilities based on their severity and potential impact on the organization. This helps security teams focus their efforts on addressing the most critical vulnerabilities first, optimizing resource allocation.
- **Reduced Human Error:** Traditional penetration testing relies heavily on manual processes, making it susceptible to human error. Testing your environment with NodeZero minimizes such errors by automating routine tasks, ensuring consistent and thorough security assessments, with the ability to compare pentest results.
- **Cost-effectiveness:** The efficiency, speed, and scalability of NodeZero can lead to overall cost savings compared to manual testing, especially for organizations with large and complex IT infrastructures.
- **Compliance Assurance:** Many industries and sectors are subject to strict regulatory compliance requirements. NodeZero helps organizations meet and exceed these standards by providing continuous and comprehensive security assessments, demonstrating a commitment to cybersecurity best practices.

Since last year's review, we consistently observe that security teams, tools, and policies all require constant tuning and enforcement. The data from last year also shows that customers who frequently attack their environment as malicious cyber threat actors would confirm that their security posture is effective. Our customers continue to do exactly that. They consistently and comprehensively assessed their individual environments using NodeZero, identified vulnerabilities, and took corrective measures to preemptively enhance their security stance and harden their attack surface.

By looking Through the Eyes of an Attacker, we have observed three predominant challenges in the past year:

- **Credentials are still the number one issue**
- **Unpatched and misconfigured software are prime targets for cyber attackers**
- **Fine-tuning security tools and staying ahead of emerging threats are imperative**

Repeatedly, we have seen these challenges permeate a customer's environment. Conversely, we've seen each of these challenges reduced when a security professional sees the results and impacts of a potential attack as an attacker would. When security vulnerabilities are not only exposed but prioritized based on what to fix first, the impacts of easily compromised credentials, exposed data, misconfigurations, poor security controls, and weak policies are made relevant and real. Those same security practitioners are now empowered to proactively thwart potential threats immediately and continuously with NodeZero.

The result is customers patching and rerunning a pentest to verify that they remediated that remote code execution (RCE) vulnerability, or revamping old password policies and Identity Access and Management (IAM) solutions to shore up weak or default credential vulnerabilities. Moreover, it allows them to fine-tune their current security tools to detect, log, alert, and stop techniques like password spray, credential dumping, brute force attacks, or credential stuffing, for example.

This report will focus on these three challenges and show you how weaknesses NodeZero illuminated and exploited over the past year led to critical impacts, deeper implications, and positive action by the customer to remediate vulnerabilities and weaknesses.

As described by Calvin Engen, Chief Technology Officer (CTO) at F12.net,

> **"I would rather have NodeZero breaching us than some nefarious actor. We are doing more than most to make sure we are keeping our ourselves and clients secure, helping bolster everyone's defenses as a result."**

HORIZON3.ai
~~TRUST BUT~~ VERIFY

CHALLENGE 1:

Credentials are Still the Number One Issue

As the trend remains from last year, cyber threat actors don't typically use sophisticated hacking tools and techniques like zero-day exploits to gain access to a network; they simply log in with legitimated user credentials. Once they gain initial access, threat actors then appear as legitimate users and can move laterally within a network to gain further access and establish persistence, steal sensitive data, bring down systems, and/or hold the organization hostage through ransomware.

We know that nefarious actors exploit credential requirements in many ways. They can:

- Take advantage of weak password strength requirements or weak account lockout thresholds
- Capture and then crack hashes
- Take advantage of accounts that reuse compromised credentials
- Use the default credentials that remain unchanged in a variety of web applications and systems processes

Highlighted by one of our customers in a recent case study,

> **"Some things like service accounts and similar had slipped through the cracks. Our IT and admin accounts were not subject to quarterly password resets, so NodeZero helped us figure out those accounts, keeping us in the know."**

But How Did They Get in to My Admin Account?

One primary reason for this issue is pre-configured default username and passwords loaded on devices and systems when they arrive from the manufacturer, often for convenience reasons during the initial setup process. Manufacturers and vendors may use generic credentials to simplify deployment, but organizations often neglect to change these defaults, assuming they provide sufficient security and that they are the only ones accessing the system. Recent publicly exploitable RCE vulnerabilities, such as Ivanti Connect Secure CVE-2024-21887, highlight that this is flawed logic, showing that attackers can exploit vulnerable software to access networks and systems remotely using stolen credentials.

Additionally, there's a tendency among administrative users to choose weak passwords or reuse the same passwords across multiple accounts, creating vulnerabilities that malicious actors can and have exploited. Also, some levels of admin or IT type accounts are not always subject to password reset or length policy requirements. This lax approach to credential management could stem from a lack of awareness about the potential risks and the importance of robust security practices.

Threat Intelligence

Credential attacks, such as Password spray, serve as a gateway for threat actors to infiltrate a system and allow for follow-on attacks. In a recent attack in 2023, state-backed threat actor Midnight Blizzard aka Nobelium utilized the password spray technique – using a list of publicly available, common weak or default credentials – to gain a foothold into targeted Microsoft systems, while enabling them to move laterally and avoiding detection. We have seen repeatedly that weak or default credentials can be the downfall of any organization regardless of size. This underscores the critical role of password spray attacks in providing malicious actors with an initial entry point, allowing them to exploit vulnerabilities and compromise the security of the targeted system.

Furthermore, some cyber threat actors may go to the extent of purchasing cleartext credentials that are accessible on the dark web. Upon obtaining initial access, these threat actors assume the guise of legitimate users, enabling them to traverse laterally within a network to acquire additional access and establish persistence. This may involve actions such as stealing sensitive data, compromising systems, or subjecting the organization to ransomware, effectively holding it hostage.

For instance, when one of our cybersecurity consulting customers launched NodeZero in their environment, it illuminated nearly **1400 discovered credentials,** with almost half in the critical category (local domain admin, local user, domain admin), allowing access to **4.6M restricted and sensitive files.** The attack path below shows injected credentials for a regular domain user account found on the network that had local administrator privileges on a machine. NodeZero was able to verify the cleartext password discovered and log into the SMB service and exploit Windows Print Spooler RCE vulnerability CVE-2021-34527 as an authenticated user with local admin privileges, leading to domain compromise, domain user compromise, and host compromise. NodeZero then loaded a Remote Access Tool (RAT) on a host using the domain admin cleartext credentials on a specific domain to enable post-exploitation by abusing CVE-2021-34527.

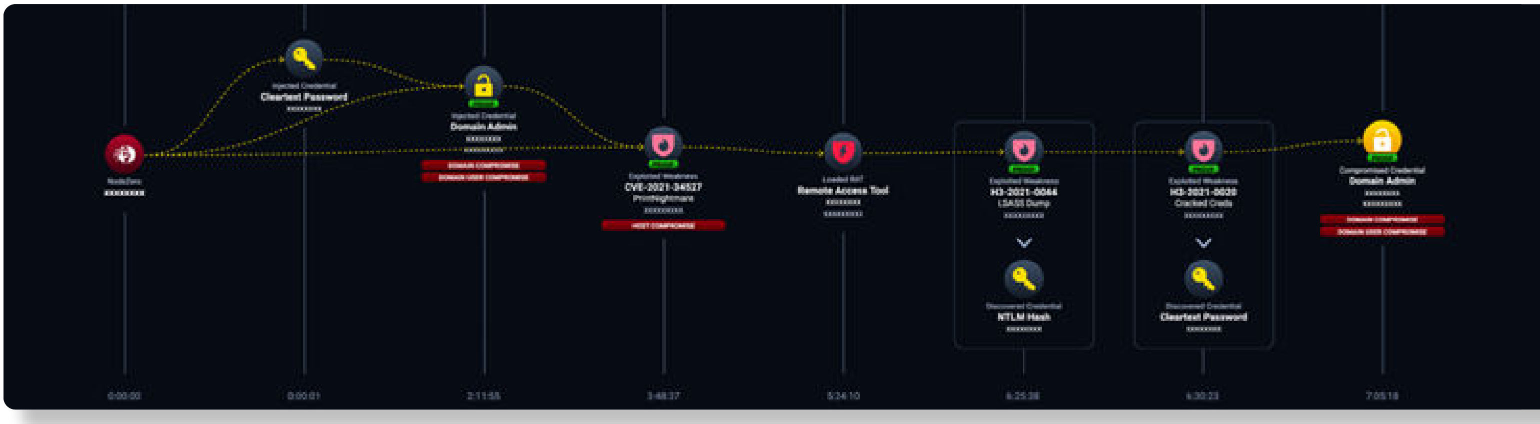


Figure 5 Attack path showing host, domain admin, and domain compromise using an injected cleartext password and the NodeZero RAT.

[1] https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/

Furthermore, NodeZero compromised the domain administrator accounts for 20+ other accounts in the domain. These accounts have unlimited access within the domain and can perform sensitive actions such as reading all employee email, accessing business data, or disabling the entire company's access to the network. This is just one example of how attackers can exploit weak or default credentials to carry out privileged actions such as dumping credentials, disabling anti-virus, and adding accounts.

Another contributing factor is the complexity of managing many credentials across various platforms and applications within an organization. With numerous systems in use, from email servers to cloud platforms and databases, administrators may struggle to enforce strong credential policies consistently. This challenge is exacerbated by employees who may resist stringent password requirements, opting for simplicity over security. The failure to implement multifactor authentication (MFA) in many instances amplifies the consequences of weak credentials. As cyber threats constantly evolve, organizations must address these issues through education, strict password policies, and the widespread adoption of MFA to mitigate the risks associated with default of weak credentials.

Implications of Credential-based Attacks

NodeZero continues to achieve critical impacts across multiple pentests within every industry, daily. These critical impacts include domain compromise, host compromise, sensitive data exposure, critical infrastructure compromise, or ransomware exposure. Addressing the impacts stemming from chained weaknesses in the customer's environment is crucial, but it's equally important to tackle the root systemic issues that contribute to these challenges. Through our interactions with customers and observations within the NodeZero portal, it is evident that numerous companies and organizations still struggle with inadequate implementation and enforcement of authentication and credential policies.

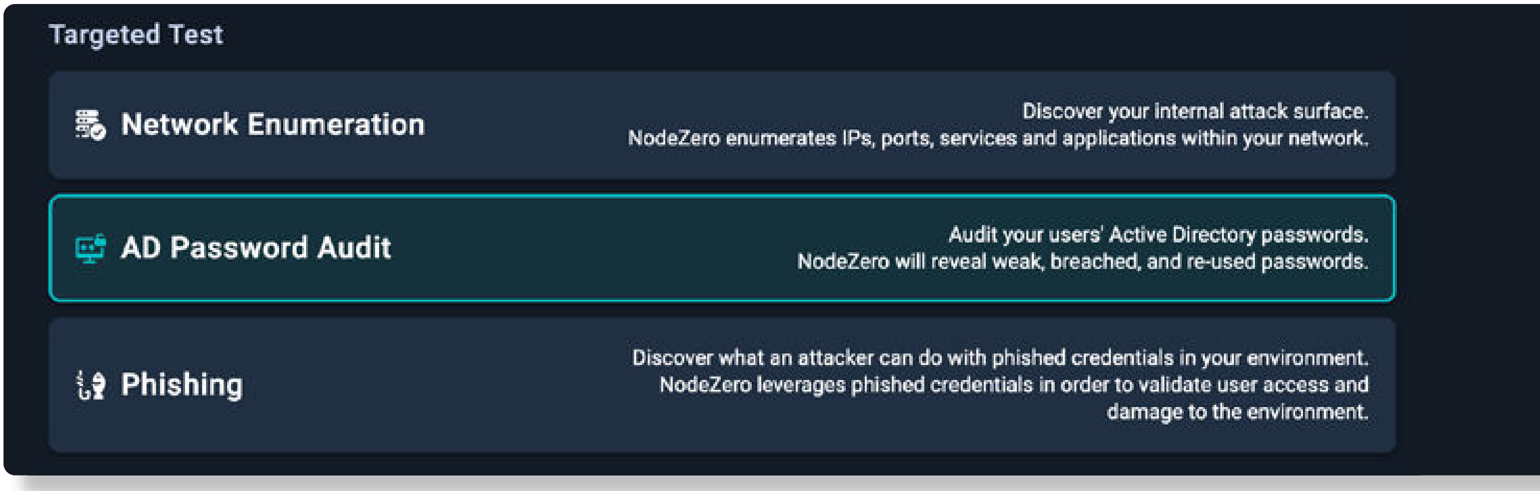
As described by one of our customers, "we thought we were doing a good job by following established IAM guidelines and policies, however, when NodeZero was introduced into our environment, we quickly discovered that's not necessarily true." It is essential to rectify these issues and implement better policies to enable a robust and resilient security environment. This also leads us to ask whether the security tools that our customers have in place are working and are effective in detecting, logging, alerting, and stopping these threats from achieving a critical impact.

Policy Recommendations and Mitigation Actions

Fortunately, there are simple changes that can be made within an organization to help prevent credential-based attacks:

- Increase training for employees on basic cyber security, including the dangers of credential reuse and weak or easily guessed passwords. Additionally, for your privileged admins, implement a Local Administrator Password Solution (LAPS) solution to help organizations prevent local admin credential reuse.
- Institute password policies that include sophistication and length requirements as described in the latest recommendations from NIST Special Publication 800-63B to include:
    - All passwords must be 12 characters or longer
    - No passwords matching the list of known breached passwords
    - No passwords derived from dictionary terms
    - No passwords derived from well-known contextual terms such as the company name, product, etc.
    - No passwords derived from well-known information about the user such as the username, first name, or last name
    - All passwords should be unique, and no passwords should be "too similar" to each other
- When creating a temporary password for a new user or a user that requires an account unlock, require the password to be used within a specific timeframe before the account becomes disabled.
- Require the use of multifactor authentication for logging into external environments and segmented networks when possible. This ensures a high degree of certainty that a cyber threat actor will not be able to gain access to public facing instances unless they also have control of the second device, such as a registered cellphone or other device to confirm a login attempt.
    - There are a variety of tools to set and enforce password policy. For instance, if you're using Azure AD, you can enable Azure AD Password Protection to automatically ban well-known bad passwords. Of note, password managers are good, but don't store your MFA tokens in your password manager!
- Implement a configuration management process that directs default credentials are changed before systems are deployed in a production environment.
- Implement good access controls to include the principle of "least privilege." Users should only have access to specific data, resources, and applications needed to complete required tasks within their role. This can help ensure that organizations are limiting their overall attack surface, while improving their security posture and reduce "over privileged" users that could misuse critical systems and increase liability.
- Disable the accounts of current or former employees who no longer require access. Oftentimes, cyber threat actors are disgruntled employees or former employees that would like to seek retribution against an organization and already have access. Disabling and not deleting the former user account allows the organization to retain any files or data that individuals may have generated while limiting the organization's risk.
- And lastly, verify that each of the above guidelines are implemented, enforced, and effective by attacking your environmental teams, tools, and rules using the NodeZero AD Password Audit or Phishing Impact test.

Figure 6 Audit your users Active Directory passwords using the NodeZero AD Password Audit test.



Targeted Test

Network Enumeration — Discover your internal attack surface. NodeZero enumerates IPs, ports, services and applications within your network.

AD Password Audit — Audit your users' Active Directory passwords. NodeZero will reveal weak, breached, and re-used passwords.

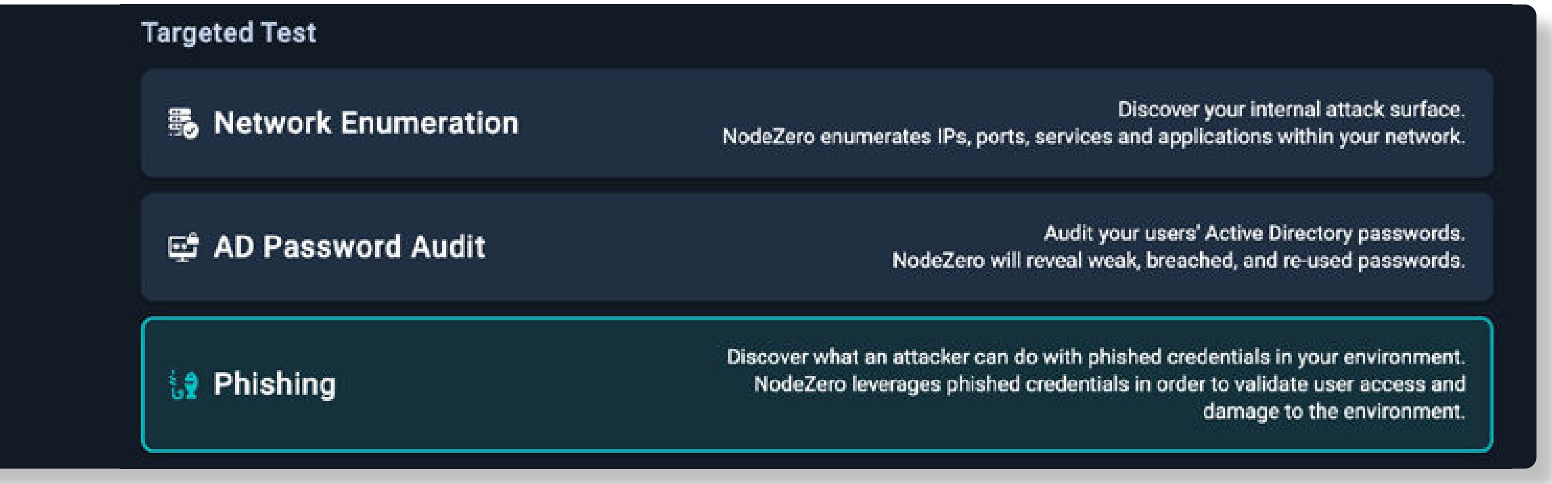
Phishing — Discover what an attacker can do with phished credentials in your environment. NodeZero leverages phished credentials in order to validate user access and damage to the environment.

More Details About AD Password Audit:

- Reveals user passwords in your Active Directory environment that are likely targets for credential stuffing, password spray, credential reuse, and password cracking attacks.
- Cracks passwords based on public breach data, open-source intelligence, and any weak password terms that you provide.
- Provides a prioritized list of risky accounts along with detailed remediation guidance.
- Enables you to regularly audit passwords as employees join or leave the organization.

More Details About Phishing Impact Testing

- Supplements your simulated phishing tools, such as KnowBe4, Proofpoint, InfosecIQ, Mimecast, and other in-house efforts.
- Interoperates with your phishing simulation solution to show the true impact of phished credentials to your business.
- Captures the credentials from the simulated phishing attack victims and uses those credentials during a NodeZero pentest against your network.



Targeted Test

Network Enumeration — Discover your internal attack surface. NodeZero enumerates IPs, ports, services and applications within your network.

AD Password Audit — Audit your users' Active Directory passwords. NodeZero will reveal weak, breached, and re-used passwords.

Phishing — Discover what an attacker can do with phished credentials in your environment. NodeZero leverages phished credentials in order to validate user access and damage to the environment.

Figure 7 Discover what an attacker can to with phished credentials in your environment using the NodeZero Phishing Impact test.

CHALLENGE 2:

Unpatched and Misconfigured Software Are Prime Targets for Cyber Attackers

Throughout the past year, numerous Horizon3.ai customers have conducted pentests, only to discover that their systems are riddled with recent exploitable vulnerabilities and some dating back several years. Astonishingly, many of these vulnerabilities have simple fixes and/or patches readily available by vendors, underscoring the critical importance of regularly updating and applying patches to ensure system security. This includes vulnerabilities from CISA's current Top Routinely Exploited Vulnerabilities list and their Known Exploited Vulnerabilities (KEV) catalog.

> **"We had just completed our own penetration test and I was super underwhelmed. Our scoring was low and there was nothing critical to report. Then we kicked off NodeZero, did a scan of our environment, and within a few hours we found a system that was not fully configured. As a result, NodeZero was able to compromise it, then move laterally through the environment, and ended up compromising our whole domain."**
>
> - Calvin Engen, CTO at F12.net

Moreover, customers often discovered that they have added software and hardware to their environments that was improperly configured and/or had default settings enabled. Software misconfigurations, if left alone, present a significant security risk to the entire environment. Most commonly, misconfigurations include default settings, insecure configurations, or overlooked security measures. Also, software misconfigurations create an environment ripe for exploitation by cyber attackers. Attackers actively search for known vulnerabilities in software configurations, leveraging automated tools and techniques to identify and exploit weaknesses.

According to the NSA and CISA, the top 10 most prevalent network misconfigurations are:

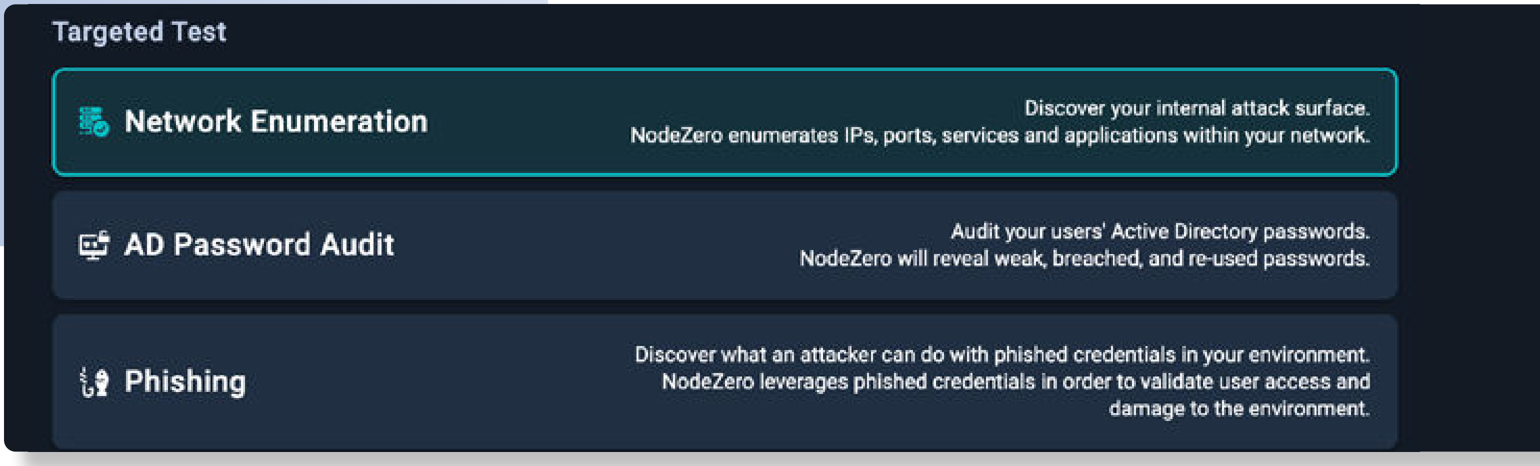
1. Default configurations of software and applications
2. Improper separation of user/ administrator privilege
3. Insufficient internal network monitoring
4. Lack of network segmentation
5. Poor patch management
6. Bypass of system access controls
7. Weak or misconfigured multifactor authentication (MFA) methods
8. Insufficient access control lists (ACLs) on network shares and services
9. Poor credential hygiene
10. Unrestricted code execution

In many cases, exploit scripts are readily available on the internet, allowing even novice attackers to launch sophisticated attacks against vulnerable systems. By exploiting misconfigurations, attackers can execute a variety of malicious activities, including unauthorized data access, privilege escalation, and system compromise. Therefore, timely patching and proper configuration management are critical to mitigating the risk posed by software misconfigurations and maintaining a secure computing environment.

It is also key to know your attack surface in and out. The NodeZero targeted Network Enumeration test serves as a critical reconnaissance technique for our customers, offering insights into an organization's attack surface by systematically discovering and cataloging network assets and services. Through the Network Enumeration test, security teams can meticulously map out their infrastructure, identifying open ports, active hosts, and network protocols.

This test helps unveil potential entry points, insufficient network segmentation, and weak spots that malicious actors could exploit to infiltrate the network, as well as any misconfigurations that need addressed. By comprehensively understanding the attack surface, our customers can prioritize security measures, fortify defenses, and proactively mitigate risks. The Network Enumeration test not only aids in bolstering the resilience of the network but also empowers security teams to stay one step ahead of adversaries by proactively addressing vulnerabilities, discovering shadow IT devices, and minimizing the likelihood of successful cyber-attacks.

▼ Figure 8 Discover your internal attack surface using the NodeZero Network Enumeration test.



Targeted Test

Network Enumeration — Discover your internal attack surface. NodeZero enumerates IPs, ports, services and applications within your network.

AD Password Audit — Audit your users' Active Directory passwords. NodeZero will reveal weak, breached, and re-used passwords.

Phishing — Discover what an attacker can do with phished credentials in your environment. NodeZero leverages phished credentials in order to validate user access and damage to the environment.

[2] https://media.defense.gov/2023/Oct/05/2003314578/-1/-1/0/JOINT_CSA_TOP_TEN_MISCONFIGURATIONS_TLP-CLEAR.PDF

The Importance of Ensuring the Security, Reliability, Resilience, and Hardening of your Landscape

Much like last year, NodeZero continues to find and exploit misconfigurations and vulnerabilities in critical DevOps tools (i.e., Jenkins, GitLab, Kubernetes, and Docker), routers, servers, Integrated Lights Out (iLOs), and Integrated Dell Remote Access (iDRACs). Compromised DevOps tools can lead to unauthorized access to sensitive code repositories, injection of malicious code into production environments, and distribution of malware, posing a significant threat to data integrity and operational continuity.

Threat Intelligence

In 2023, DevOps Tools such as Jenkins, GitLab, Kubernetes, and Docker still have security vulnerabilities and are targeted due to their widespread usage in software development and deployment.

For instance, in Mar 2023 Jenkins encountered severe security issues related to plugin vulnerabilities allowing a threat actor to initiate cross-site scripting (XSS) attacks and gain unauthorized access and complete compromise of the Jenkins server[3].

GitLab also faced similar security challenges in the past year, when a financially motivated operation dubbed LABRAT, enabled an attacker to use stealthy and defensive evasion in their attacks. The attacker utilized undetected signature-based tools, sophisticated and stealthy cross-platform malware, command and control (C2) tools which bypassed firewalls, and kernel-based rootkits to hide their presence. Moreover, the attacker used a legitimate service, TryCloudFlare, to obfuscate their C2 network[4].

To mitigate these types of vulnerabilities in DevOps tools, it's crucial for organizations to stay informed about the latest security advisories and to implement security best practices such as regular patching, least privilege access controls, network segmentation, and container image scanning can help strengthen DevOps pipelines and containerized environments. Additionally, leveraging security tools and running NodeZero continuously harnesses the **Find, Fix, Verify loop,** identifying and remediating potential vulnerabilities before malicious actors exploit them.

[3] https://thehackernews.com/2023/03/jenkins-security-alert-new-security.html

[4] https://sysdig.com/blog/labrat-cryptojacking-proxyjacking-campaign/

Similarly, vulnerabilities in networking components can grant attackers unauthorized access, control over network traffic, and the ability to disrupt essential services, compromising confidentiality, availability, and integrity of the network. NodeZero users are keenly aware of the importance for them to promptly address these misconfigurations to mitigate potential cyber threats and ensure the security, reliability, resilience, and hardening of their IT infrastructure.

For example, one of our major customers in the food and beverage arena discovered an authentication bypass and execution of code vulnerability in their HPE iLO 4 instance (CVE-2017-12542), leveraged in 6 additional attacks paths leading to Host Compromise. NodeZero also highlighted that this vulnerability led to 5 critical downstream impacts and the discovery of cleartext 'local administrator' password, with access to the SSH service.

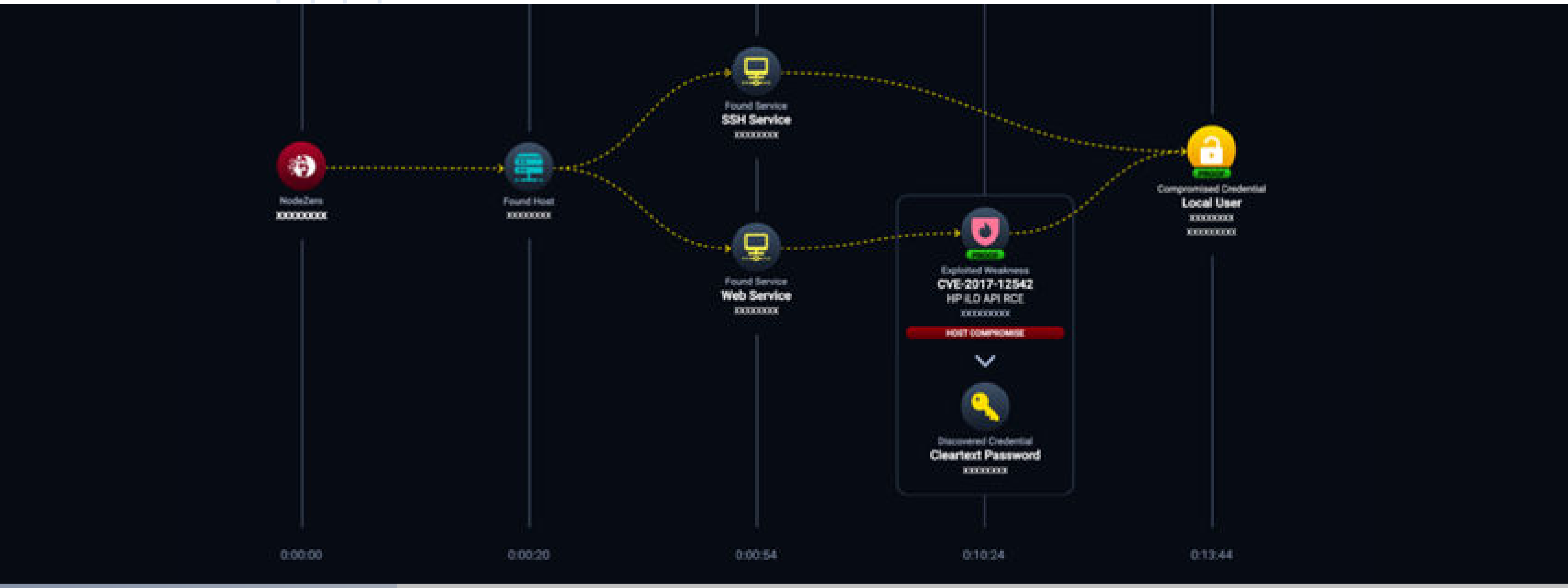


Figure 9
Attack path shows NodeZero leveraging CVE-2017-12542 and discover local admin cleartext password leading to host compromise.

Using iLO allows admins to power servers on and off, restart servers, measure power usage, apply patches, and access event logs of a system. Unauthenticated attackers with access to the HP iLO Web API can gain control of the vulnerable server, as well as viewing the cleartext passwords of all users. Further, host compromise can lead to attackers gaining access to sensitive information, maintaining persistence within your network, and obtaining lateral movement within your networks. While many companies or organizations may choose to leave their servers unpatched, Horizon3.ai customers are realizing the consequences of this and are urged to protect against the bypass of authentication.

Legacy Systems Continue to Remain a Threat

Although NodeZero keeps pace with emerging threats, legacy vulnerabilities still plague organizations every day. This is especially true when NodeZero users running legacy systems and software in their environment discover vulnerabilities dating back to 2008 that are still being exploited by threat actors. As we have seen, many organizations struggle to keep up with the constant stream of security patches and updates released. Legacy systems may be difficult to patch due to compatibility issues or because they are no longer supported by vendors, creating a window of opportunity for attackers to exploit known vulnerabilities.

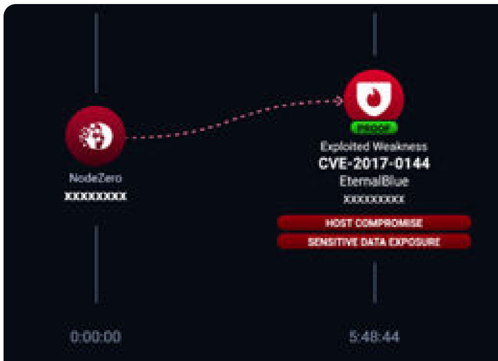
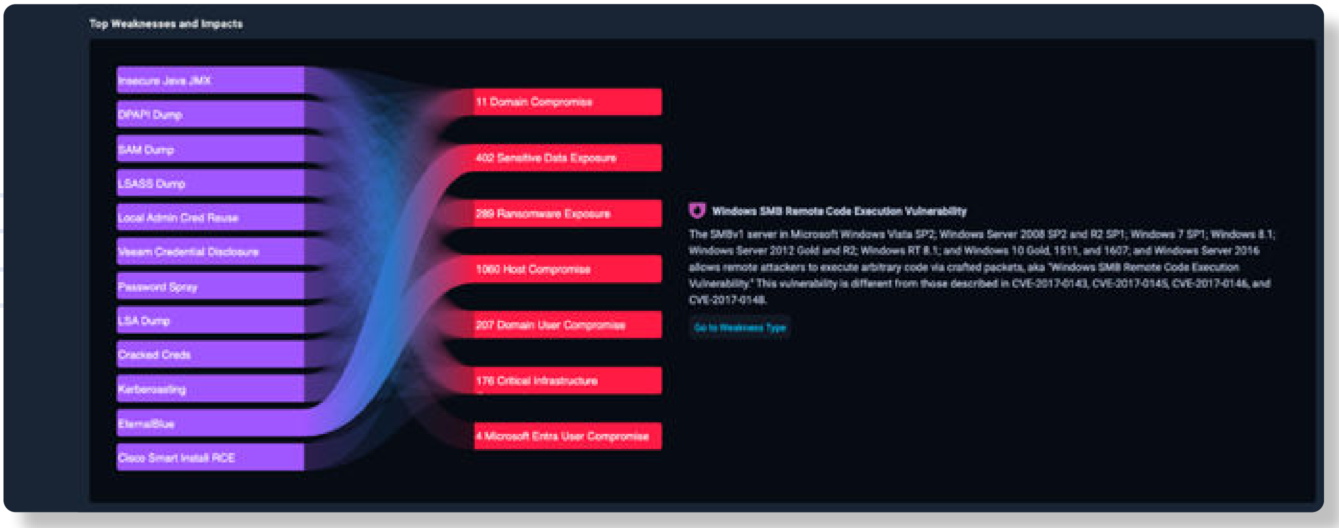


Figure 10 Attack path shows NodeZero discovery of CVE-2017-0144 leading to host compromise and sensitive data exposure.

For example, NodeZero discovered EternalBlue CVE-2017-0144 multiple times in one of our cybersecurity services partner environments, leading to host compromise and sensitive data exposure to ~14M protected files. EternalBlue is a legacy Windows SMB RCE vulnerability that exists when the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests. An attacker can exploit the vulnerability by sending a specially crafted packet to the SMBv1 server. This would then give the attacker the ability to execute code on that targeted SMBv1 server. As we saw in a recent test [Figures 10 & 11], EternalBlue was leveraged by NodeZero and used to achieve host compromise and sensitive data exposure impacts across the entire network. Host compromise can lead to attackers gaining access to sensitive information, maintaining persistence within your network, and obtaining lateral movement within your networks, while sensitive data exposures can be used to obtain user credentials, personally identifiable information (PII), financial account data, and other business-critical information to further exploit or gain profit.



Windows SMB Remote Code Execution Vulnerability

The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.

Figure 11 Sankey chart highlights top weaknesses and impacts, showing that EternalBlue led to 402 sensitive data exposure and 1060 host compromise impacts.

Fortunately for our customer, NodeZero found the vulnerability before an attacker could target their network/systems and provided them with mitigations to prevent such an attack from occurring in the future. In this instance, they were directed to apply the updates referenced in Microsoft Security Bulletin MS17-010 and block access to SMB services from untrusted networks such as the Internet, as well as disabling SMBv1 if possible.

Threat Intelligence

Old CVEs such as EternalBlue (CVE-2017-0144) and BlueKeep (CVE-2019-0708) remain relevant due to their persistence in unpatched or legacy systems and their potential for widespread exploitation. Despite patches being available for these vulnerabilities, many organizations fail to apply them promptly, leaving systems vulnerable to exploitation. Cyber threat groups, including but not limited to nation-state actors like the North Korean Lazarus Group and Russian APT28 (Fancy Bear), have utilized EternalBlue for high-profile attacks such as the WannaCry ransomware outbreak in 2017 and various campaigns targeting critical infrastructure and government entities. Similarly, BlueKeep has been exploited by threat actors like the Chinese Hafnium group to compromise vulnerable systems and launch subsequent attacks. These examples underscore the ongoing relevance of old CVEs and the critical need for organizations to prioritize patch management and security updates to mitigate the risk of exploitation.

Implications of Failures to Patch and Misconfigurations

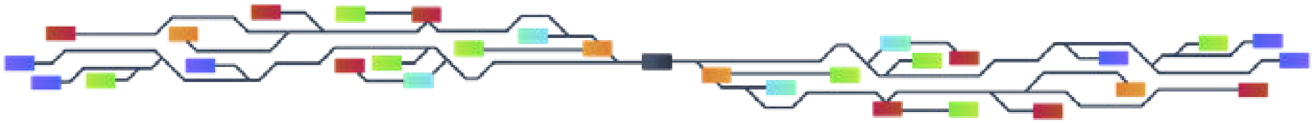
When NodeZero exploits these vulnerabilities and misconfigurations as an attacker would, especially when they are strung together to reach critical impacts, it tells us a few things about the organization and its environment:

1. Companies and organizations may be having trouble implementing patching policies that keep their systems up-to-date, and that previous vulnerabilities remain unmitigated. Some of the vulnerabilities we briefly discussed are over five years old, have been found on multiple machines, and have published vendor fixes and/or mitigation actions readily available. All organizations need to do is apply the patches or mitigation actions and confirm they are fixed.

2. The customer may also be having difficulty prioritizing what needs to be fixed. The organization's security team might be spending time patching and fixing vulnerabilities that may not actually be exploitable within their environment or have a lower criticality than those that will lead to critical impacts like host compromise, domain compromise, or ransomware exposure. Meaning, they aren't prioritizing and fixing what actually matters.

3. An organization may have legacy systems that are not able to be patched to the latest version, because of certain incompatibility issues with other technologies on the network. In those cases, the systems that cannot be upgraded or patched need to be segmented from the rest of the environment. This will limit any impact that a threat actor would have if it were able to exploit the vulnerability on that specific machine.

4. IT departments may have issues configuring new hardware like routers when adding them to the network. Too often we find that customers discover new hardware was added to their network with default settings and passwords that are made available on the open web, making it easily exploitable for any nefarious actor who would come across it.



Policy Recommendations and Mitigation Actions Misconfigurations

When it comes to preventing cyber threat actors from taking advantage of known vulnerabilities and weaknesses, Horizon3.ai recommends instituting patching and mitigation policies to keep your systems as up to date as possible. We recognize that not all technologies can be patched due to the risk of disrupting other components within the environment. In those cases, we recommend implementing vendor-approved fix actions and mitigation strategies to prevent the vulnerability from being exploited in your environment. If those fix action or mitigation strategies are still not available to you, we recommend segmenting that machine from the rest of your environment to prevent a malicious actor from reaching other portions of your environment and achieving critical impacts.

Of course, we do not suggest patching or implementing fix actions and merely moving on. Instead, organizations need to verify that those patches and fix actions were implemented correctly and effectively. We suggest running a regular cadence of autonomous pentests with NodeZero within your environment to do just that. In doing so, NodeZero can find those exploitable vulnerabilities and weaknesses that may still be in your environment, fix those vulnerabilities and weaknesses, and verify that the fix and mitigation actions were successful. Further, by continuously running this **Find, Fix, Verify loop,** security professionals are also able to keep abreast of any changes to ensure that those same (or new) exploitable vulnerabilities and weaknesses don't creep into the environment.

CHALLENGE 3: Fine-Tuning Security Tools and Staying Ahead of Emerging Threats Are Imperative

Did we detect it? Did we alert on it? Did we stop it? Did we log it?

A recurring sentiment voiced by Horizon3.ai customers is the frustration surrounding their investment in Endpoint Detection and Response (EDR) solutions. Many express dissatisfactions with spending considerable resources on EDR solutions, only to find that they did not detect, alert, stop, and log the right actions immediately. Such inefficiencies prompt questions about an organization's capacity to identify malicious actors, efficiently log events, promptly alert cybersecurity personnel, and prevent threat actors from carrying out malicious activities.

We consistently see that it is not necessarily the tool itself that failed, but rather it is a failure of configuring the tool properly.

This understanding emerges as our customers adopt an attacker's perspective through NodeZero. Customers gain actionable insights into the TTPs employed by threat actors, such as Man-in-the-Middle attacks (NTLM relay) or privilege escalation vectors (Kerberoasting), along with crucial data like timestamps, to uncover exploits and attack paths pointing to how threat actors could achieve significant impacts. When our customers continuously assess their cyber environment with NodeZero, it allows them to gain an understanding into emerging threats, vulnerabilities, and attack patterns, thereby enabling them to fine-tune their current cybersecurity suite effectively. This can also help pinpoint areas where current cybersecurity tools are falling short or where additional protections are needed to mitigate risks effectively.

Moreover, continuous assessments provide valuable data and feedback loops that empower our customers to optimize the configuration, performance, and efficacy of their cybersecurity tools. By correlating findings from their pentests with real-world security incidents and threat intelligence, they can refine detection thresholds, update rule sets, and implement proactive defenses to better detect, alert, prevent, and respond to cyber threats. This iterative process of implementing NodeZero to help empower customers in fine-tuning cybersecurity tools ensures that they remain aligned with evolving threats and organizational needs, while enhancing overall security posture and resilience against cyber attacks.

HORIZON3.ai
~~TRUST BUT~~ VERIFY

Research and Development Enables Readiness and Resilience

In tandem with in-house vulnerability research and exploitation, our engineers and researchers use comprehensive industry information (i.e., CISA, NIST, and/or similar) to prioritize and enhance NodeZero's attack content.

Additionally, Horizon3.ai takes a targeted approach to new zero-day and N-day threats as they emerge through our rapid response alerts, allowing our customers to test whether they are impacted and preemptively secure against them. Our teams also conduct thorough open-source research to determine what vulnerabilities are actively being exploited by threat actors in the wild and what vulnerabilities may impact our customers. When we identify high value vulnerabilities, the Horizon3.ai Attack Team often reverse-engineers them and creates proof-of-concept (PoC) exploits to enable NodeZero to demonstrate the true impact of the vulnerability in your network.

As explained by one of our customers, Art Ocain, Airiam's CISO & Strategic Alliances and Incident Response Product Management Lead, "the idea of the attack team keeping everything completely up to date when there's a new vulnerability [CVE] release while also doing their own PoC and building it into the system" is a game-changer. "You're not going to see other products turning a vulnerability into an exploit in less than a month… that blew me away," he added.

Why does this matter to our customers? The in-depth research and development conducted by our teams empower any user of NodeZero to take back their network, allowing them to be ready for and stay ahead of attackers.

> **"Think of NodeZero as a Resiliency Test for your Organization"**
>
> **Art Ocain, CISO at Airiam**

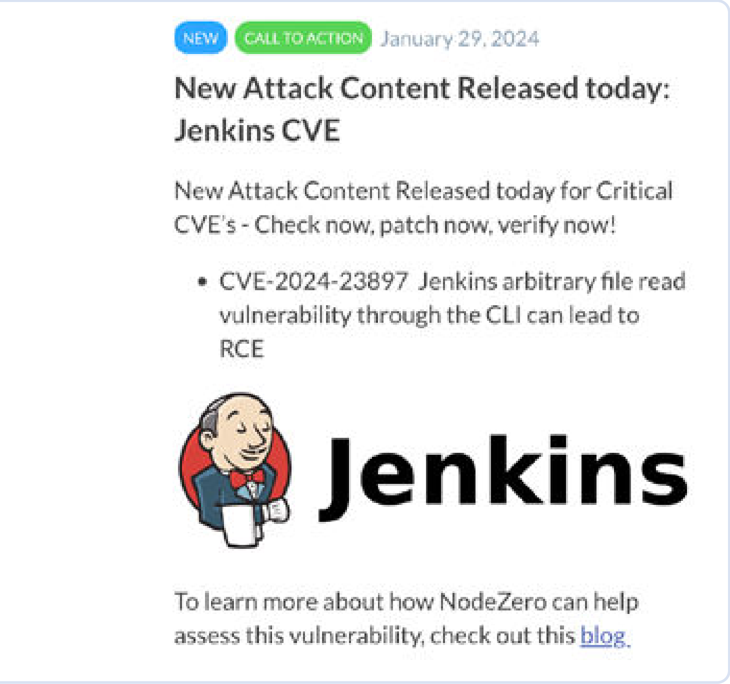
Rapid Response Program

Zero-Day vulnerabilities drive fear within the cyber community, because they often have a severe impact due to their unknown nature. Adversaries can take full advantage of exploiting Zero-Day vulnerabilities until they are discovered and disclosed publicly, and patches or mitigation measures are developed and made available.

Conversely, N-Day vulnerabilities often pose a much larger threat because they may or may not have readily available fix actions but are publicly known and leave organizations exposed until patches or mitigations are shared. According to Dark Reading[5], “N-day vulnerabilities are a goldmine for attackers because the hard work has already been done.”

Horizon3.ai is keenly aware of the threat both Zero-Day and N-Day vulnerabilities pose to our customers, which is why we created rapid response alerts to combat such dangers. Our Rapid Response alerts aim to:

1. Quickly integrate Zero-Day and N-Day attack content into NodeZero
2. Proactively identify and notify our prospects, customers, and partners that are likely at risk or known to be exploitable
3. Enable those customers the ability to run a targeted pentest to verify they are no longer exploitable or quickly run a retest to verify the issue has been remediated
4. Work with our partners to ensure they continue to be positioned as trusted advisors to their customers



January 29, 2024

New Attack Content Released today: Jenkins CVE

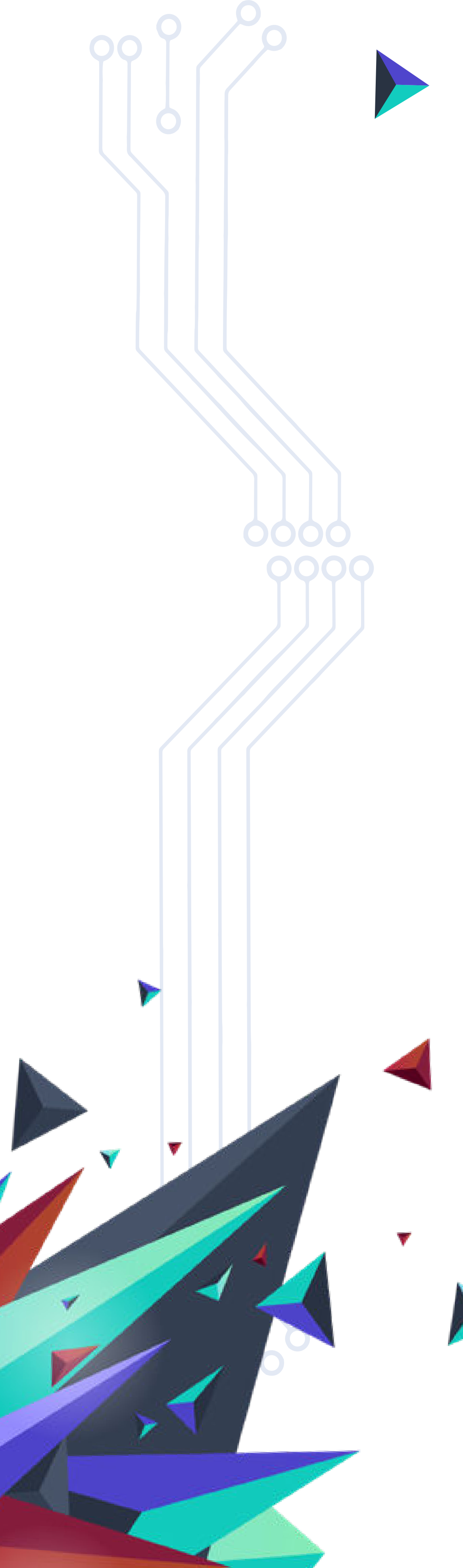
New Attack Content Released today for Critical CVE's - Check now, patch now, verify now!

- CVE-2024-23897 Jenkins arbitrary file read vulnerability through the CLI can lead to RCE

To learn more about how NodeZero can help assess this vulnerability, check out this blog.

We often alert our customers to newly released vulnerabilities through our rapid response notifications. These notifications focus on any potentially exploitable instances in their environment while including the availability of patches and fix actions to remediate the weakness, and the ability to run a pentest to verify that the corrective actions were successful. We also ensure that our customers stay up to date on any developments on the specific vulnerability, such as the ongoing exploitation by malicious cyber threat actors in the wild. This not only facilitates cybersecurity professionals with a full understanding of what vulnerabilities are being actively exploited in their environment, but what fix actions to take first to mitigate threats proactively.

[5] https://www.darkreading.com/vulnerabilities-threats/the-overlooked-problem-of-n-day-vulnerabilities



Implications and Policy Recommendations

As customers continue to proactively illuminate their environments by running a regular cadence of pentests and utilizing the **Find, Fix, Verify loop,** we often find that their security teams still ask why NodeZero was able to achieve critical impacts when they have security tools in place that should be able to stop the threat. This implies that the security team was unable to proactively detect, alert, stop, and log threats before they materialize with the security tools they have in place.

Although we do not recommend or endorse any other specific cybersecurity tools beyond NodeZero, companies should conduct thorough research and evaluation. They should identify their specific security needs, considering factors such as the size of their organization, the complexity of their IT environment, and the types of threats they are most concerned about or that NodeZero has discovered and exploited. Also, companies should assess EDR solutions based on key criteria such as detection capabilities, real-time monitoring, response automation, and integration with existing security infrastructure. It's crucial to evaluate the accuracy and efficacy of threat detection algorithms, the speed and granularity of alerting mechanisms, and the comprehensiveness of response actions offered by the EDR tool.

Additionally, companies should consider factors like ease of deployment, scalability, vendor support, and regulatory compliance requirements. Further, they should conduct thorough testing and pilot programs to ensure that the selected EDR tool aligns with their security objectives and effectively addresses their threat landscape. Regular updates, continuous monitoring, and ongoing optimization are essential to maximize the effectiveness of EDR tools in proactively identifying and mitigating security threats.

Conclusion

We have seen that Horizon3.ai customers of all sizes have found exploitable critical vulnerabilities, misconfigurations, and weaknesses in their environments thanks to NodeZero.
We have also seen that these vulnerabilities, misconfigurations, and weaknesses consistently fall into three general themes:

1. Weak or default credentials and poor policy enforcement, not sophisticated exploits, lead to most of the common weaknesses experienced by our customers. Credential-based attacks are the most common method for cyber threat actors to gain a foothold in your environment, and yet are often easily fixed.
2. Unpatched and misconfigured software remains a prime target for threat actors to exploit. Companies and organizations should continuously implement patching policies to ensure that their environment is up to date and resilient, while also confirming that their environment is configured properly and hardened against cyber-attacks.
3. Cybersecurity tools require proper oversight and fine-tuning to be effective, especially when up against emerging threats like Zero-Day and N-Day vulnerabilities.

It is not enough to simply employ security tools and think that they will prevent the next cyberattack without regularly assessing the efficacy of those tools in your environment using NodeZero. Companies and organizations that constantly ensure that their cybersecurity tools are configured properly enable their security teams to proactively detect, alert, stop and log a threat before it's too late.

We have consistently found that taking the hacker's perspective by continuously attacking our own environments with NodeZero and running the Find, Fix, Verify loop is essential to understanding if we are truly secure or not.

NodeZero permits our customers to take the necessary steps to prioritize and fix or mitigate those vulnerabilities, misconfigurations, and weaknesses that lead to critical impacts. This includes pointing our customers to the latest patches and mitigation actions by individual vendors. Once the vulnerabilities are believed to be fixed or mitigated, our customers are then asked to run another pentest or 1-click verify. This ensures that the fix actions and mitigation steps were applied correctly.

OVER THE HORIZON

What's Next for NodeZero?

As cybersecurity professionals, we believe we should always be iterating, learning, and adapting to illuminate and combat new threats. Our approach to building NodeZero is no different.
Our teams at Horizon3.ai are constantly working to proactively assess the ever-changing cyber threat landscape, while also integrating customer feedback and developing new content. In 2024, we will remain committed as we put out new Internal and External attack content, iterate on our targeted pentest options (Network Enumeration, AD Password Audit, and Phishing), and strive to deliver a best-in-class overall user experience for our customers.

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

HORIZON3.ai
~~TRUST BUT~~ VERIFY