HORIZON3.ai

~~TRUST BUT~~ VERIFY

WHITE PAPER

Five Key Outcomes of Continuous Security Assessments in Manufacturing

Manufacturing

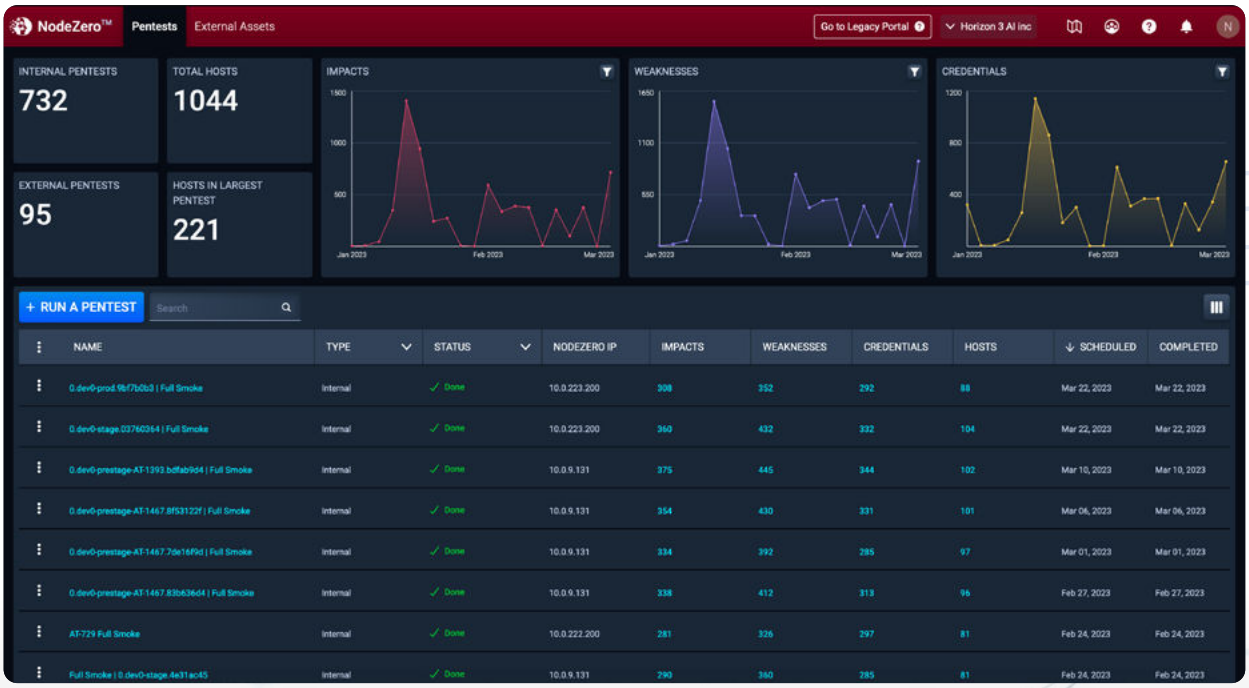
 @Horizon3ai info@horizon3.ai www.horizon3.ai

Five Key Outcomes of Continuous Security Assessments in Manufacturing

How Autonomous Pentesting Helps Manufacturers Assess and Reduce Risk

Historically, manufacturers have been susceptible to a variety of obstacles, including stiff competition, an inability to modernize quickly, and government-imposed regulation, among others. Until recently, manufacturers were largely happy to produce goods with little concern about "information-based threats." But all that has changed. Manufacturers, like many others, have adopted new Information Technology (IT), Operational Technology (OT), Internet of Things (IoT), and a host of other technologies modern manufacturing businesses need to succeed in today's business climate.

At the same time, the cyber threat landscape is now rife with attackers who want to take manufacturers offline, hold them for ransom, and impede their business and brand. In terms of resiliency and business continuity planning, the computing devices running offices, factories, machinery, and all other processes that streamline operations introduce new levels of considerable risk. Due to the recent ransomware attacks against organizations in every industry, never has the risk of falling victim been higher for manufacturers.



Enter NodeZero™

Due to the continuous threat against the manufacturing sector, Horizon3.ai delivers the **NodeZero** platform which helps manufacturing organizations continuously assess themselves, discover critical issues, and validate security improvement over time. NodeZero is designed to let you see and test your networks from an attacker's perspective with its autonomous pentesting approach.

The defensive cybersecurity technology you have deployed in your manufacturing environment may help block an attack from the outside-in. Unfortunately, none of that same technology highlights where the attack paths are in your networks. To solve that problem, we specifically developed NodeZero. It highlights where exploitable vulnerabilities and weaknesses exist in your networks, explains how to fix them quickly, then verifies your fix worked.

For example, a major global manufacturer that provides commercial, industrial, and municipal water solutions has adopted an aggressive and proactive approach to validating security controls and policies using NodeZero. By bringing Horizon3.ai's autonomous pentesting solution in house, this organization strengthened and hardened their cybersecurity posture over time, at both speed and scale.

With a team of just 2 IT security engineers, the manufacturer initiated over 12k hours of completely automated pentesting using NodeZero. Historically running only 1 or 2 pentests per year, the manufacturer has now completed 320+ pentests to date since their adoption of the NodeZero in mid-2021 in an environment with ~12k hosts. According to the manufacturer, this effort has significantly reduced their cyber risk.

By adopting a purple team culture, the organization has been able to use NodeZero both as a sparring partner and as an internal auditor for their stack of security tools and infrastructure policies and procedures.

> **Through a regular cadence of NodeZero tests, the IT security team conserves time tuning the identification, logging, alerting, and blocking of malicious threats across their SIEM/SOAR solutions, EDRs, and other defensive tools.**

Additionally, NodeZero helped spearhead an infrastructure audit for a recently completed merger and acquisition (M&A). By conducting a pentest of the soon-to-be-acquired organization, the buying organization proactively identified and mitigated new risks before finalizing the merger. Post M&A, these organizations seamlessly merged IT infrastructures and now all hosts and assets are held to the same security standards. The savings in terms of risk and time reduction to complete the necessary due diligence of the merger were significant.

Elevated Level of Risk

As the cyberthreat landscape continuously changes, manufacturers face a unique set of IT challenges, as well as the real, physical ramifications that impact their bottom lines. Today's attackers fully understand the disadvantages manufacturers face, especially in terms of their reliance on various computing systems, antiquated operating systems, commercial and custom-built applications, and lots of devices – some new and some incredibly old.

Simply put, attackers who gain remote access to any internal computing device are the primary threat manufacturers face. Once an attacker achieves access, they use it to take over networks and ransom critical systems. If successful, operations cease until the ransom payment is made and received.

According to an IBM study, the average cost of a ransomware attack – not including the cost of the ransom itself – is USD 4.54 million.

In comparison to a natural disaster, fire, or other similar incident, a cyber event like ransomware that halts production is just as critical to plan for, especially in terms of risk management and business continuity. And the key to remediating risk is to continuously assess your own part of the cyber world, detect your potential attack paths, and fix what matters most. The results can be dramatic in terms of cybersecurity improvement.

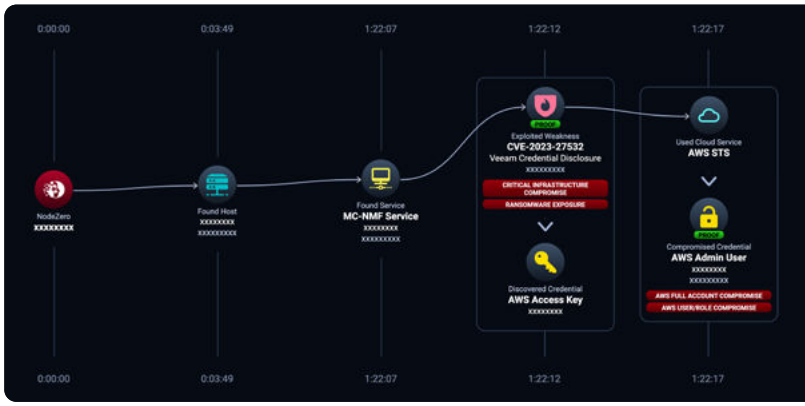
Companies like FM Global, who provide insurance to manufacturers, encourage their customers to advance their security culture and clearly identify business risks, including cyber risks. This means conducting proper security risk assessments to see where weaknesses are and working with industry experts to fix them. Insurance companies clearly understand the value of risk assessments and risk remediation.

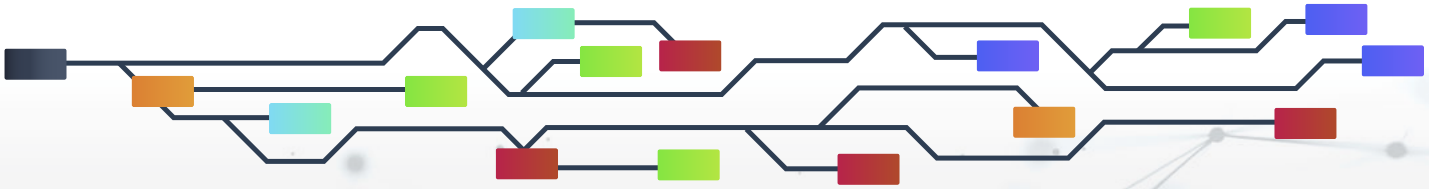
Attack Paths Explained

In the context of cybersecurity, attack paths provide a graphical representation of the possible paths an attacker can take to exploit weaknesses in your computers, servers, applications, infrastructure, and security controls. An attack path assessment highlights weak credentials in use, discovers software misconfigurations, identifies known application vulnerabilities, and finds dangerous product defaults.

There are two ways to discover attack paths – post attack and pre attack. In the context of a post attack, forensic experts identify them after attackers complete their mission. They highlight what an attacker did, and often, experts must make some assumptions. This type of analysis is an important after-the-fact exercise, but it will not protect you from the consequences of an attack.

In today's world of offensive security approaches, discovering pre-attack paths is imperative before they become a reality. This reduces risk, improves resiliency, and helps ensure business continuity. Therefore, solutions that can safely, accurately, and continuously conduct assessments of your critical infrastructure and networks, discover your attack paths, provide remediation guidance, and ensure security improvement is made are highly desired in manufacturing and all other industries.





HORIZON3.ai
~~TRUST BUT~~ VERIFY

An Example Attack Path

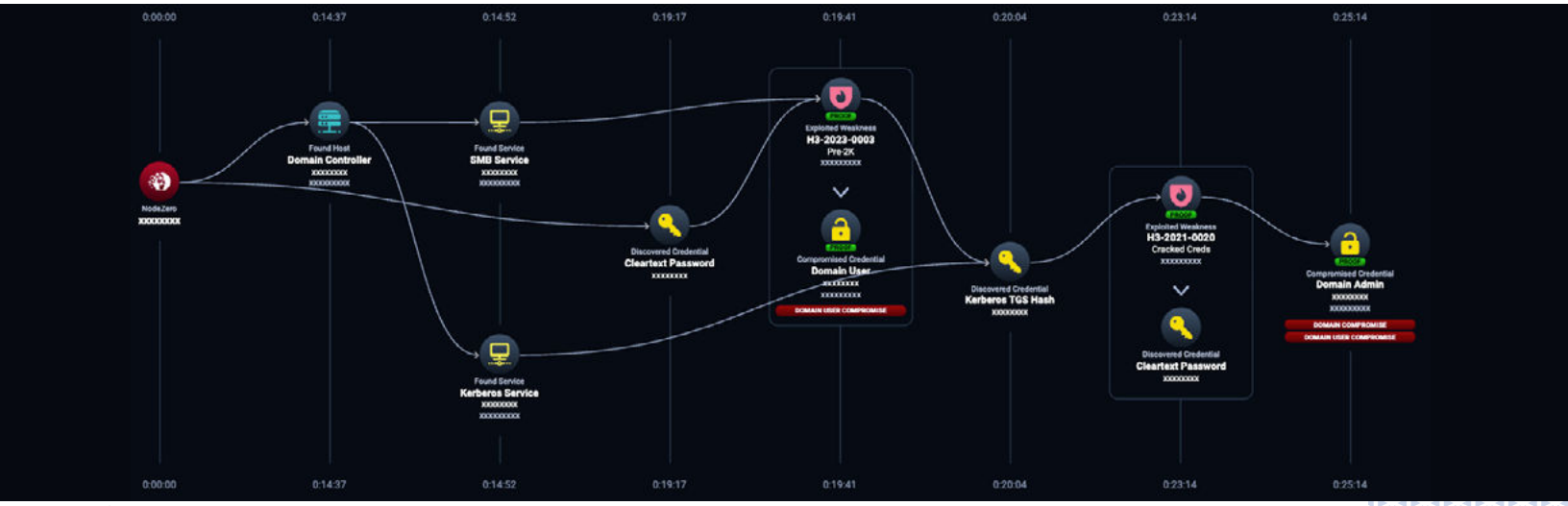


Figure 1

Although some attack paths are quite complex, others are remarkably simple to understand. For example, Figure 1 is an attack path that came from a NodeZero pentest. In this case, NodeZero simulated an attacker who had gained a foothold in a company's production network.

> **Once NodeZero started its operation, it was fully capable of proving that it had compromised a domain in the organization and became a domain admin in ~25 minutes.**

What is also interesting about the attack path in Figure 1 is that NodeZero **discovered H3-2023-0003: Pre-Windows 2000 Computer Set** (see top middle of Figure 1) affecting the credential for a certain domain user.

Then, NodeZero verified the credential for a domain user by exploiting H3-2023-0003: Pre-Windows 2000 Computer Set. A few steps further, NodeZero's attack resulted in Domain Compromise and Domain User Compromise. (See far right.)

NodeZero found a computer in this network running a pre-Windows 2000 operating system, exploited it, and eventually achieved domain admin. In the context of manufacturers, they likely have some older computers still in use that are running operating systems no longer supported. Although the older computers work just fine for the minimal tasks they perform, they can be an enabler of a successful domain takeover.

Once a domain is fully compromised, all hosts, domain user accounts, data, infrastructure, and applications tied to that domain should be considered fully compromised. In this case, and many others like it, once an attacker becomes a domain admin, they can easily download data, plant ransomware, encrypt critical systems, and hold an organization for ransom.

To Defeat Ransomware, You Must Know Where You're at Risk

Ransomware is one of the most primitive cyberattacks, yet it's one of the most effective and destructive. It is very proficient at interrupting operations for an extended period and is capable of permanently taking an organization like yours offline – especially if you refuse to pay up. So how does human-operated ransomware work?

First, attackers must establish a foothold in your network by compromising a computing device, then maintaining remote access to that device for some interval. Gaining a foothold often involves a simple phishing email where an employee clicks on something, attackers exploit an RCE vulnerability in a public-facing system, or they take advantage of weak or default passwords in a networking device that's exposed. Regardless of how it's done, attackers achieving a foothold is always the first step.

Attackers don't need to hack in – they log in. From our observations, attackers are using credential-based attacks far more often than exploiting known CVEs. For example, in 2022,

> **NodeZero successfully executed credential-based attacks over 6,000 times in our customers' networks without exploiting a single CVE.**

After they achieve a foothold, attackers then use that device as a launch point since they are remotely controlling it, normally right through your perimeter firewalls. Then, attackers begin their attack path by finding critical network systems like domain controllers, database stores, essential applications, and so on.

Once attackers find these systems, they use dozens of possible methods to gain admin privileges. Then attackers proceed to steal your data until you meet their demands or attackers install Locker ransomware to lock you out of critical systems. Attackers may also use Crypto ransomware to encrypt important files and databases, and only provide the decrypt key once you have paid the ransom.

CrowdStrike's 2023 Global Threat Report shows adversaries are doubling down on stolen credentials, with a 112% year-over-year increase in advertisements for access-broker services identified in the criminal underground. In other words, attackers are gaining remote access into many organizations' networks, and are selling that remote access to ransomware gangs.

An example of this is the June 2023 MOVEit Zero-day vulnerability, where the CL0P ransomware gang, otherwise known as Lace Tempest, is credited with initially exploiting the vulnerability and publishing an extortion note on its dark web leak site claiming to have information on hundreds of businesses.

The most effective way to defeat ransomware-based attacks is to continuously assess your own infrastructure, find the attack paths an attacker would take, and then fix those issues and validate that your fixes defeated the discovered attack paths. Once complete, you rinse and repeat the process regularly to discover new attack paths. No other defensive or offensive method of reducing the risk of ransomware will be as successful as the method explained here.

The Need for Continuous Assessments

No two networks are the same, and with the continuous rise in technology consumption, and the evolution of technology and modernization in manufacturing, often no two days are the same. In fact, manufacturers have become victims of the latest appliance, sensor, piece of machinery, process technology, and/or computing approach since they must integrate antiquated technologies with modern technologies – and the outcome presents many unknowns that increase risk.

As a result, a previous cyber risk assessment from a year ago only provides value if it is still valid, but when something changes in the network, or you infuse some recent technology into a run-of-the-mill process, the previous assessment no longer provides a complete picture of your risk. Bringing in consultants for a few days to assess your security posture is unfortunately a one-and-done task that's expensive, time consuming, and provides little return on your investment.

Manufacturers vastly need a continuous assessment approach that adapts as they grow and innovate. When something changes in their environment, they can automatically perform a new assessment. As employees come and go due to headcount turnover, running additional assessments makes sense too. But the whole point of assessments is they need to become second nature – automated in the same fashion as your manufacturing processes. This is where NodeZero delivers.

Benefits of Continuous Assessments

Automating NodeZero into your daily workflows delivers a clear understanding of your risk exposure – one that will provide clarity and engagement with your leadership team. You will be able to show how you're defending the organization and justify your investment in cybersecurity. And that investment is not onerous – NodeZero costs around the same as a single, manual, scoped down pentesting engagement. With NodeZero, you can assess yourself all day, every day for no additional costs.

The benefits of continuous assessments defeat the unknowns and deliver confidence that security is improving daily. No longer will IT and security teams struggle to understand where they are most at risk. Instead, they will have a clear picture of their security posture at any given time. In addition, armed with reports, data points, trends, analysis, and identified attacks paths, NodeZero will help streamline remediations for understaffed IT departments who are also responsible for security.

Five Key Outcomes of Continuous Assessments

Understanding the reasoning behind a continuous assessment approach – that will improve security – is imperative. In context of this approach, here are the expected outcomes and benefits:

1 Reduce cyber risk

You can discover, triage, and eliminate new attack paths that put your organization at risk of a successful ransomware attack. And when using NodeZero, scheduling continuous assessments of your infrastructure and mitigating issues found is the most reliable and truly effective way of reducing cyber risk.

2 Prevent expensive outages

You can prevent costly production downtime, defeat data theft, decrease regulatory penalties, and avoid reputational damage. Using the findings and detailed remediation guidance from NodeZero, you can eliminate costly post-breach investigations while maintaining uptime and meeting production demands.

3 Decrease security costs

You can lessen cybersecurity costs and preserve valuable IT person-hours. With NodeZero, you can perform continuous penetration testing assessments with no hardware or agents to buy or install, and you can eliminate the need to perform disruptive manual assessments or hire expensive 3rd party assessors or pentesters.

4 Improve security posture

You can reduce time to remediation with contextual prioritization, so you spend time fixing what matters most and avoid focusing on non-exploitable vulnerabilities. Running NodeZero daily results in increased security, identifies systemic issues, and ensures streamlined and effective security initiatives.

5 Measure security improvement

You can receive highly detailed reports and trending data to prove progress and improvement of your security program. Using NodeZero to help track progress ensures you are getting a return on your investment, while proving that you're adhering to security best practices, industry guidelines and recommendations, and safety requirements.

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

HORIZON3.ai
~~TRUST BUT~~ VERIFY

Mandatory Security Assessments

Coming Soon

Considering the widening cyber threat landscape, the increase in money-motivated threat actors, and the recent successful ransomware attacks against supply chains, it is becoming increasingly important for manufacturing, state and local government agencies, healthcare, education, finance, critical infrastructure, and other industries to take securing their cyber environment seriously.

For example, in the proposed – or active – regulations or guidelines below, each call for assessments in the context of leadership security skills, continuity and resiliency, and overall cybersecurity readiness. Governments understand the critical role technology plays and recognize the importance of assessments.

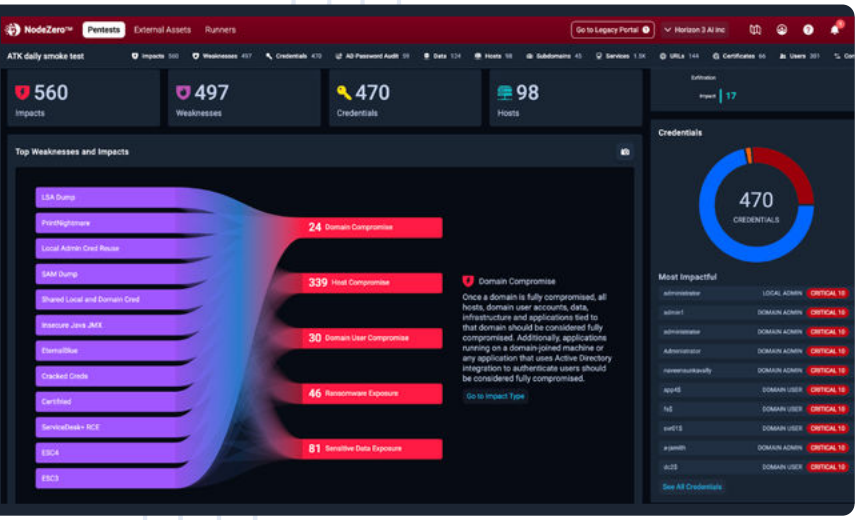
- SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies
- The Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554
- The NIS2 Directive: A high common level of cybersecurity in the EU
- DOD Issues Final Rule Updating Supplier Performance Risk System (SPRS) Assessment Procedures for Federal Contractors
- NIST Special Publications 800-171r2 - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Although there are many more references to regulations and guidelines available, the overarching theme is clear. If you are a publicly traded entity, do business with governments, or are part of critical infrastructure, you will need to perform continuous security assessments, then provide proof of current (not past) levels of security.

More About the Benefits of NodeZero

Organizations, including manufacturers, who have adopted NodeZero as part of their risk assessment process, and added it into their cybersecurity programs, experience the following benefits, and more.

Eliminate risks and validate security with continuous assessments. Provides proof of current security levels, highlights effective remediations, tracks improvement over time, and generates reports that analysts and auditors understand.



Improve security performance and visibility of their risk level. Delivers reports that leaders will appreciate and verifies risks are identified, prioritized, and addressed, plus justifying their investment, and proving its effectiveness.

Spot attack vectors before they're exploited through easy-to-understand attack paths. Proactively identifies weaknesses and provides top-level views of larger systemic issues, and how to address them at a macro level for long-term cyber resilience.

Obtain a prioritized list of what needs fixing most urgently. Eliminates time-consuming false positives and improves the capacity of security and IT teams regardless of the level of expertise or size of the overall team.

Perform assessments on demand. Allows teams to find, fix, and verify as often as they like – and even concurrently – without additional costs while reducing the need to hire 3rd party assessors and penetration testers.

What NodeZero discovers daily in networks just like yours confirms what we have always known. To fully understand what would happen if an attacker gained a foothold in your network, you must continually attack your own environment the same way they would. NodeZero enables organizations of all sizes to safely attack themselves as often as they like.

Final Comments From HORIZON3.ai

~~TRUST BUT~~ VERIFY

We recognize the dilemma all manufacturers face. You must innovate and use technologies to their fullest capabilities to streamline your operations. If not, you cannot compete in a global marketplace. However, the threat of ransomware and other cyberattacks has never been higher.

We believe you should be able to use all technology available to ensure your success, and our goal is to help you do that more safely. **NodeZero reduces risk, maintains uptime, and meets the demands of manufacturers of all sizes.**

- **To test drive NodeZero in your own manufacturing environment, sign up for a free trial soon.**

https://www.horizon3.ai/trial

- **To learn how NodeZero can help secure your manufacturing business, schedule a demo today.**

https://www.horizon3.ai/demo

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

HORIZON3.ai

~~TRUST BUT~~ VERIFY