HORIZON3.ai

~~TRUST BUT~~ VERIFY

WHITE PAPER

Fortifying the Chain: A Proven Strategy for Supply Chain Defense

Supply Chain

Fortifying the Chain: A Proven Strategy for Supply Chain Defense

Understanding the Landscape of Cyber Threats and the Innovations in Third-Party Risk Management

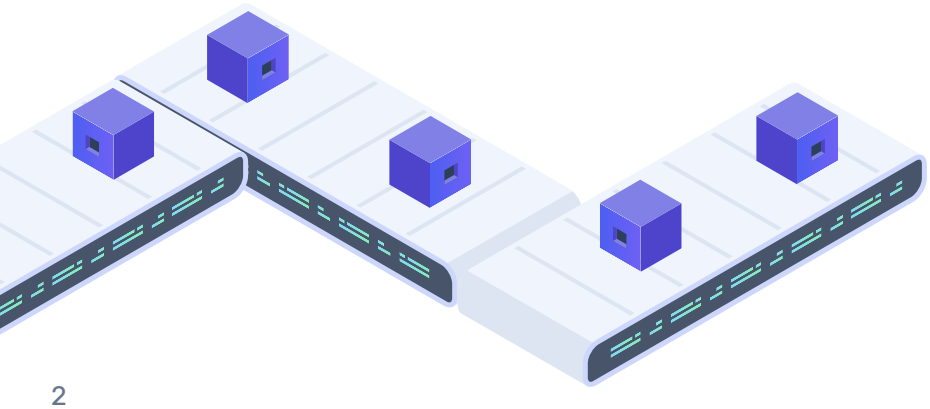
Today's cyber attackers are well aware that targeting smaller companies which supply components, parts, software, and services to upstream buyers can cause significant disruptions to the supply chain. Since buyers depend on these smaller suppliers for timely delivery of goods, any network disruptions leading to production outages can severely affect the sustainability of buyers upstream.

Board-level supply chain risk is becoming more visible as attackers increasingly focus their efforts on these smaller suppliers, who are often the weakest link. Consequently, this poses a significant threat to the operational integrity and business continuity of organizations, making it a critical issue for CEOs, COOs, and CISOs to address promptly.

In this whitepaper, we delve into the evolving landscape of cyber threats targeting the supply chain, highlighting the increasing vulnerability of smaller suppliers to sophisticated cyberattacks. We explore the strategic methodologies attackers use, including leveraging open-source intelligence (OSINT) to pinpoint and exploit weaknesses within the supply chain, thereby posing significant risks to operational integrity and business continuity.

A focal point of our discussion is the introduction of **NodeZero™ for Third-Party Risk Management**, an innovative solution designed to mitigate these risks through autonomous penetration testing and continuous assessment. We detail the process of identifying, assessing, and prioritizing suppliers for security enhancements, alongside real-world case studies that underscore the critical nature of robust supply chain defense mechanisms.

Through these discussions, the paper aims to equip CEOs, COOs, and CISOs with a proven strategy to fortify their supply chains against cyber threats, ensuring operational resilience and maintaining trust with partners and customers.



HORIZON3.ai
~~TRUST BUT~~ VERIFY

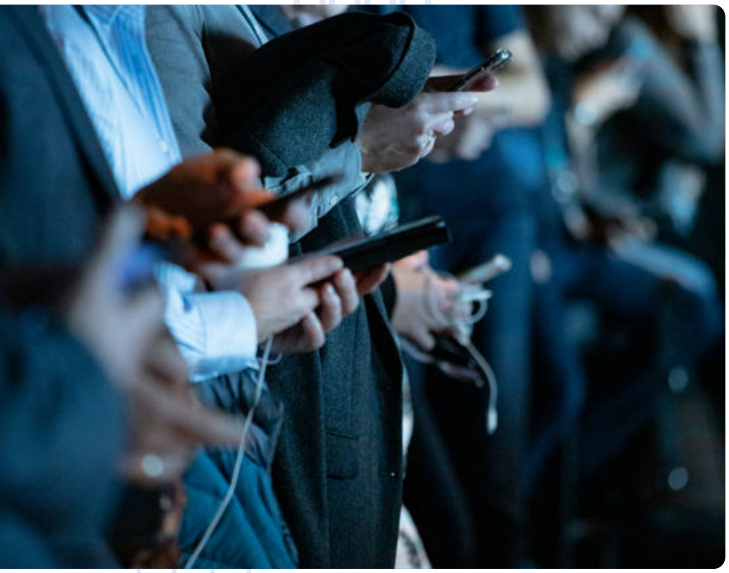
Table of Contents

HORIZON3.ai
~~TRUST BUT~~ VERIFY

Critical Nature of the Problem

The interconnectedness of supply chains means a cyber-induced outage at one point can lead to significant disruptions, financial losses, and reputational damage upstream. In today's just-in-time (JIT) and lean manufacturing environments, ensuring the security of the supply chain is not just about protecting data, but also about maintaining business continuity and trust with partners and customers.

The reality is that your exploitable attack surface is not just your own IT infrastructure any longer, but the IT infrastructure of your suppliers and your distributors too. Since this is clearly the case, let's define the steps attackers may take to identify the most vulnerable and impactful targets within a supply chain, leveraging OSINT and other strategic criteria for target selection.



How Attackers Use OSINT in Identifying Their Targets

Open-source intelligence (OSINT) is a critical tool for attackers in the initial phases of a supply chain attack. By exploiting publicly available information, attackers can map out a target organization's supply chain, identify key suppliers, and gather actionable intelligence without arousing suspicion. Today's attackers utilize various OSINT sources, including social media, corporate websites, regulatory filings, and more, to build a comprehensive understanding of a target's supply chain network.

Techniques for Effective OSINT Gathering

Attackers employ a range of techniques for OSINT gathering, from automated web scraping to manual searches of industry forums and news sites. Advanced OSINT tools and search engines are also utilized to filter through vast amounts of data quickly. The effectiveness of OSINT reconnaissance lies in the attacker's ability to synthesize disparate pieces of information into a coherent picture of the supply chain landscape.

How Attackers Strategically Select Their Targets

The strategic selection of suppliers to target in a supply chain attack is a sophisticated process that leverages extensive intelligence and a nuanced understanding of the supply chain's dynamics. Beyond OSINT, applying other specific criteria for target selection enables attackers to maximize the harm they can inflict on organizations.

Criticality to the Supply Chain

One of the primary criteria for target selection is the supplier's criticality to the upstream organization's operations. Attackers prioritize suppliers whose disruption would have the most significant impact, considering factors such as the uniqueness of the supplier's product or service, the difficulty of replacing the supplier, and the overall effect on the supply chain.

Vulnerability Assessment

Beyond criticality, attackers assess the vulnerability of potential targets. This involves analyzing the supplier's cybersecurity posture, including the presence of known vulnerabilities and weaknesses, the effectiveness of existing security measures, and the potential for remaining undetected. Attackers look for targets with weak security practices, outdated infrastructure, or a history of security incidents.

Potential for Downstream Impact

Attackers also consider the potential for downstream impact when selecting a target. Suppliers with extensive networks or those integral to multiple organizations' supply chains are particularly attractive, as disruptions can cascade, affecting a wide range of entities and maximizing harm.

Visibility and Reputation

The visibility and reputation of the supplier within the industry play a role in the selection process. Attacking a well-known, reputable supplier can amplify the perceived impact of the attack, eroding trust across the supply chain and potentially leading to broader destabilization beyond the immediate operational disruptions.

Case in Point: Toyota's Supply Chain Attack and Outcome

In 2022, a cyberattack on Kojima Industries, a Toyota parts supplier, underscores the significant impact that supply chain vulnerabilities can have on global corporations and economies. The attack on the single supplier significantly impacted Toyota, forcing it to halt operations at 14 factories, leading to an estimated loss of about $375 million. This incident demonstrates the interconnected nature of modern industries where a cyberattack on a single supplier can lead to substantial financial losses and operational disruptions. It serves as a critical reminder of the importance of cybersecurity vigilance across all levels of the supply chain.

Other Examples of Supply Chain Incidents

- Okta Supply Chain Attack (October 2023)
- JetBrains Supply Chain Attack (September/October 2023)
- MOVEit Supply Chain Attack (June 2023)
- 3CX Supply Chain Attack (March 2023)
- Applied Materials Supply Chain Attack (February 2023)
- Fantasy Wiper Supply Chain Attack (December 2022)
- Visser Supply Chain Attack (February 2020)

The Role of Autonomous Pentesting in Improving Suppliers' Security

In response to these sophisticated threats, autonomous penetration testing emerges as a crucial defensive tool. By simulating the tactics, techniques, and procedures (TTPs) of real-world attackers, autonomous pentesting solutions like NodeZero from Horizon3.ai provides organizations and their supply chains with a proactive means of identifying and mitigating vulnerabilities and weaknesses before they can be exploited

Being safely launched from within suppliers' network infrastructures, NodeZero finds exploitable weaknesses and vulnerabilities they may not know exist. It then prioritizes the issues it discovers so suppliers can remediate such risks. NodeZero then verifies any discovered issues have been remediated well before they become critical risks to the supply chain, ensuring resiliency and business continuity are maintained.

For CEOs, COOs, and CISOs: Strategic Benefits of NodeZero for Third-Party Risk Management

NodeZero for Third-Party Risk Management is a proven approach aimed at mitigating cyber risks. It offers a continuous assessment platform that allows for regular self-assessment of suppliers' IT security. This strategy enhances JIT and lean manufacturing processes by efficiently assessing suppliers' cyber defenses, reducing effort for suppliers, and maximizing risk mitigation for buyers. Benefits include:

- **Business Continuity:** NodeZero ensures that suppliers' systems are resilient against attacks, helping to maintain continuous production flows essential for JIT and lean manufacturing models.
- **Risk Management:** A robust cybersecurity posture becomes part of the company's risk management strategy with NodeZero, aiding in the prevention of unforeseen costs associated with cyber incidents.
- **Operational Efficiency:** NodeZero's autonomous penetration testing reduces the need for extensive in-house security teams, pentesting consultants, and specialized skills, aligning with lean operational principles.
- **Competitive Advantage:** A secure supply chain is a reliable one, and this reliability translates into a competitive advantage as clients and partners trust organizations that prioritize end-to-end cybersecurity.
- **Compliance and Reputation:** Using advanced tools like NodeZero demonstrates due diligence in cybersecurity practices, helping organizations meet regulatory compliance standards and bolster their reputation.

Made for Modern Reliance on Supply Chains

NodeZero for Third-Party Risk Management provides an essential layer of security assessment for those who are dependent on third-party suppliers that deliver a product or offering that buyers rely on.

This reliance is particularly clear in the high-stakes environment of JIT and lean manufacturing. Consequently, ensuring that the manufacturing sector can maintain the integrity and reliability of their value chains is critical. By integrating NodeZero into their supply chain security strategy, CEOs, COOs, and CISOs can protect their operations from cyber threats and maintain the seamless flow that is critical to their success. This same approach can be applied in other industries as follows:

Example Scenarios:

- A financial institution, through continuous assessment using NodeZero, tracks security improvements in its software vendors, ensuring compliance and securing customer data.

- A healthcare provider uses NodeZero to continuously assess its pharmaceutical suppliers, quickly identifying and addressing exploitable vulnerabilities before an attack can impact operations.

- A manufacturing company identifies a critical component supplier with a high-risk score due to outdated systems. After assessment and vulnerability remediation via NodeZero, the supplier's risk score improves, bolstering supply chain security.

HORIZON3.ai
~~TRUST BUT~~ VERIFY

Benefits of Horizon3.ai's Approach

NodeZero for Third-Party Risk Management offers a multi-faceted approach to identifying and mitigating supplier-related cyber risks:

Identifying Weak Links: Utilizing OSINT and external asset discovery, NodeZero evaluates suppliers, assigning risk scores to those likely to be targeted by attackers.

Prioritizing for Onboarding: Organizations can prioritize their suppliers for continuous security testing based on calculated risk scores, ensuring efforts are effectively allocated to bolster supplier security.

Automating Onboarding and Training: Streamlines the integration of selected suppliers into the NodeZero platform, complemented by comprehensive training to ensure effective utilization of the autonomous penetration testing solution.

Providing Continuous Security Posture Reporting: Offers detailed, ongoing insights into the security posture of suppliers, allowing for real-time visibility and strategic response to emerging threats.

Why Suppliers Would Participate

Suppliers have compelling reasons to engage in this approach:

Extended Security Responsibility: Recognizing that their security posture now extends beyond their individual organization, participation in this sort of approach would enhance not just their own security but strengthens the whole ecosystem in which they are a part of.

Arms-Length Relationship Management: Horizon3.ai works closely with organizations and their suppliers, guiding them on how to ensure that only pertinent security information is shared, maintaining confidentiality while enabling necessary transparency.

Evolving Vendor Risk Requirements: As larger companies overhaul their vendor risk assessment protocols to necessitate thorough security testing and reporting, suppliers would be motivated to comply to maintain these essential business relationships.

NodeZero for Third-Party Risk Management: **Use Case**

It's clear that traditional cybersecurity measures and approaches, when used in some supplier environments, can fall short in effectively identifying and mitigating exploitable risks. Often, security best practices are deprioritized in smaller supplier settings, mainly due to the absence of dedicated security-focused personnel, inadequate security budgets, and leaders not fully understanding their risks. A common refrain is, "We're just a small supplier. Why would anyone target us?"

Aware of this credible concern, a US Department of Defense (DoD) Agency, which relies heavily on the Defense Industrial Base (DIB) Sector, proactively developed a program centered on NodeZero for Third-Party Risk Management. The purpose of this initiative was to motivate suppliers to assess their infrastructures, identify exploitable risks, remediate these risks, and thus ensure that risk was not transferred to the DoD Agency. The DoD Agency funded the overall program.

The Approach That Worked Best

The DoD Agency first identified critical SMB and mid-market suppliers that posed the highest operational risks and collaborated with Horizon3.ai to onboard these suppliers onto the DoD Agency's instance of the NodeZero platform. This process involved:

Focused Identification: The DoD Agency selected suppliers critical to operational integrity and provided that list to Horizon3.ai.

Automated Onboarding: Horizon3.ai managed the onboarding and integration of selected suppliers into the NodeZero platform.

Comprehensive Training and Support: Horizon3.ai provided tailored training and ongoing support to the DoD Agency to enable effective use of the platform by supplier teams.

Continuous and Automated Testing: Suppliers utilized the NodeZero platform's capabilities to conduct regular, autonomous penetration tests to identify and remediate exploitable vulnerabilities.

Automated Reporting: The DoD Agency received continuous reports on the current state and on improvements in the security posture of their suppliers.

HORIZON3.ai
~~TRUST BUT~~ VERIFY

Notable Positive Outcomes and Risks Reduced

- One DIB firm completed 70+ bi-weekly pentests with NodeZero in the last four months with limited effort other than to set up and launch the tests.
- Another DIB firm conducted its first external pentests two days after onboarding, and NodeZero proved it could exploit a known vulnerable software product in their network.
- Another DIB firm discovered that NodeZero was able to gain access to testing data, manuals, and other sensitive information stored in the firm's network.

Results of Using NodeZero Within the DoD Agency's Supply Chain

The initiative demonstrated significant improvements in the cybersecurity resilience of the DoD Agency's supply chain, notably:

Reduced Vulnerabilities: A measurable decrease in critical vulnerabilities across onboarded suppliers, reducing the overall risk profile of suppliers and the DoD Agency itself.

Operational Continuity: Enhanced security measures led to a marked improvement in operational resilience, with fewer disruptions, lower risk, and more predictable outcomes.

Strategic Insights: Automated reporting provided actionable insights, allowing for targeted improvements and better resource allocation.

Increased Collaboration: The process fostered a collaborative security culture, with suppliers more engaged in proactive cybersecurity practices.

Note: The DoD Agency mentioned above continues to expand their coverage, bringing more suppliers into the program daily.

HORIZON3.ai
~~TRUST BUT~~ VERIFY

More About NodeZero for Third-Party Risk Management

NodeZero reveals the attack paths for every weakness it discovers, detailing each step an attacker could take to penetrate supplier defenses. It uncovers blind spots in suppliers' security posture that extend beyond known CVEs and patchable vulnerabilities, such as easily compromised credentials, exposed data, misconfigurations, poor security controls, and weak policies. Weaknesses are prioritized based on their impact, allowing suppliers to understand what to fix first. NodeZero also offers detailed guidance to aid supplier remediation efforts. Here are a few additional benefits provided by NodeZero:

- **Assessing a Wide Range:** NodeZero evaluates on-premises infrastructures, external attack surfaces, cloud services, identity and access management systems, data infrastructures, and more.
- **Chaining Attack Vectors Autonomously:** NodeZero navigates through networks laterally, linking weaknesses just as an attacker would, and then exploits them safely – demonstrating proof of exploitation.
- **Prioritizing Threats:** NodeZero determines which weaknesses are truly exploitable and critically impactful, helping suppliers rank their remediation efforts. It also highlights systemic issues, enabling the remediation of many weaknesses with a single fix, such as policy adjustments.
- **Operating Without Agents or Special Hardware:** NodeZero is a self-service SaaS platform that runs safely in production environments. It doesn't require any maintenance of hardware or software, nor does it need persistent or credentialed agents.
- **Allowing Continuous, Unlimited, and Coordinated Deployments:** NodeZero enables suppliers to enhance their security effectiveness, scheduling and running numerous pentests on their largest networks and even conducting multiple pentests simultaneously.
- **Conducting Autonomous Operations:** The NodeZero platform continuously expands its operations to assist suppliers in assessing and validating their security posture, including internal pentesting, external pentesting, AD password audits, Phishing Impact testing, and N-day testing.

HORIZON3.ai
~~TRUST BUT~~ VERIFY

Conclusion

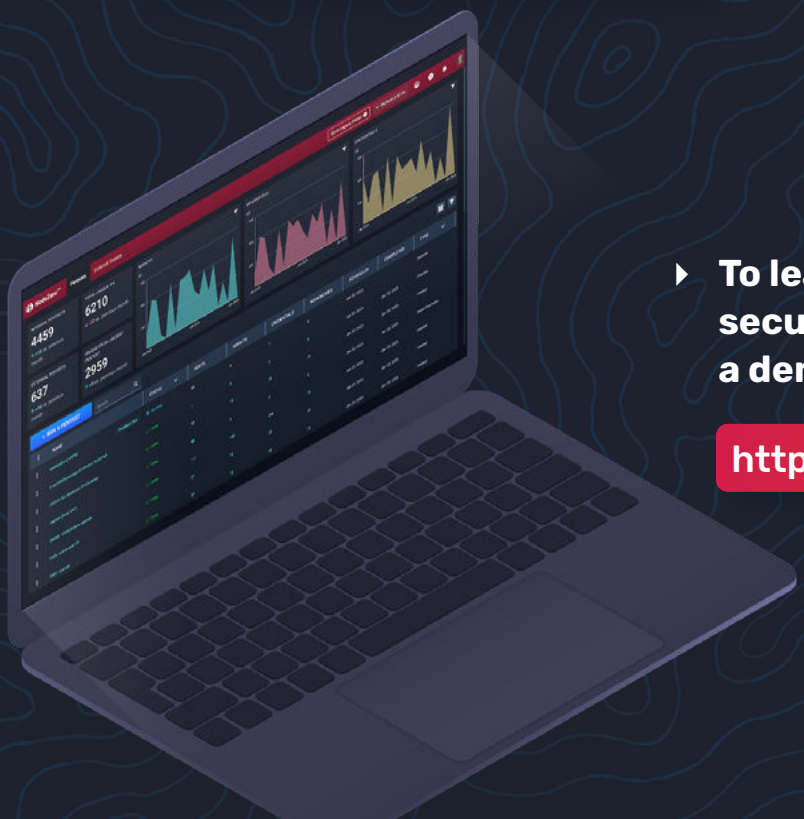
The rapidly evolving cyber threat landscape necessitates a robust and proactive approach to supply chain security. **NodeZero for Third-Party Risk Management** stands at the forefront of this challenge, offering an innovative and forward-thinking solution that is indispensable for the defense of complex supply chains.

By implementing this platform, organizations are not only able to comprehensively assess and address vulnerabilities within their supply networks but also enhance their overall resilience against cyber threats. The strategic value of NodeZero extends beyond immediate security—it is a catalyst for strengthening operational reliability, safeguarding critical data, and ensuring the continuity of business operations in an era where the supply chain is a critical artery for organizational health.

Through continuous vigilance and advanced penetration testing, NodeZero empowers businesses to stay one step ahead, transforming supply chain security from a potential liability into a steadfast competitive edge.

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

https://www.horizon3.ai/trial



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

https://www.horizon3.ai/demo