Enhancing Cybersecurity Through Collaborative Risk Management

Use Case About NodeZero™ for Third-Party Risk Management

Traditional cybersecurity measures and approaches can fall short in effectively identifying and mitigating exploitable risks. Often, security best practices are deprioritized in some 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:

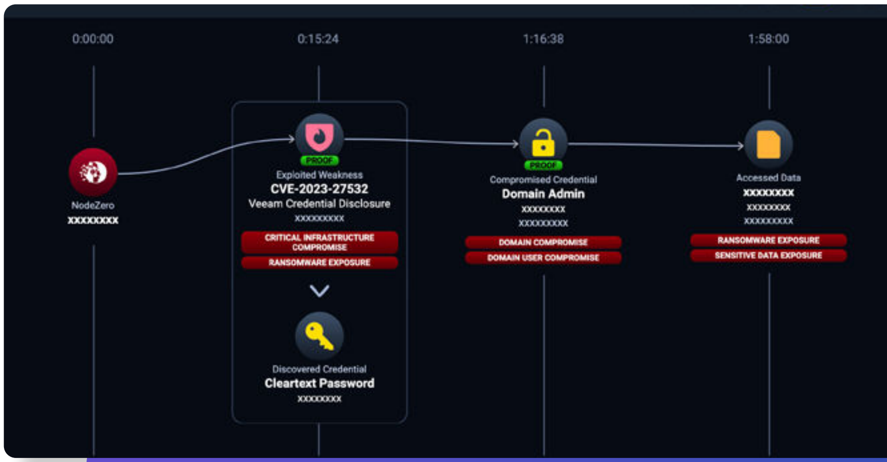
Reduced Vulnerabilities: A measurable decrease in critical vulnerabilities across onboarded suppliers, reducing the overall risk profile of suppliers and the DoD Agency itself.

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 continues to expand their coverage, bringing more suppliers into the program daily.



*NodeZero obtained **Infrastructure Compromise** and **Domain Compromise** in this supplier's network. NodeZero also identified **Ransomware Exposure** and **Sensitive Data Exposure** in less than 2 hours.*

Conclusion

The initiative to implement **NodeZero for Third-Party Risk Management** represents a significant step forward in enhancing cybersecurity within the Defense Industrial Base (DIB) Sector. By addressing the common and often overlooked security shortcomings among suppliers, the DoD Agency has not only strengthened its own security framework but has also elevated the security posture of its suppliers.

The collaboration with Horizon3.ai has led to a robust and proactive cybersecurity environment characterized by continuous and automated testing, immediate vulnerability mitigation, and operational resilience. The results speak for themselves with a reduction in vulnerabilities, improved operational continuity, strategic insights, and an increase in collaborative security culture.

HORIZON3.ai
~~TRUST BUT~~ VERIFY