info@Horizon3.ai
www.Horizon3.ai
LinkedIn: Horizon3.ai
Twitter: @Horizon3ai

Best Practices

Catch Up, Keep Up, Stay Ahead Approach

The **Best Practices** feature is an analysis of the operational outcomes and other data found during a **NodeZero** operation that indicates whether or not your network is aligned to industry best practices and frameworks. Leveraging both successful and unsuccessful tactics, techniques and procedures from an attacker's perspective provides insight on what you seem to be doing well and where improvement is needed.

Our goal is to help organizations **Catch Up, Keep Up, and Stay Ahead** with proactive security.

Catch Up, Keep Up, Stay Ahead Approach

☐ ***Catch Up:***

- Accept that attackers know more about your environment than you do.
- Vulnerable ≠ exploitable – criticality is a function of exploitability and potential business impact.
- Assess your enterprise, determine criticality of findings, and fix the problems that matter.

☐ ***Keep Up:***

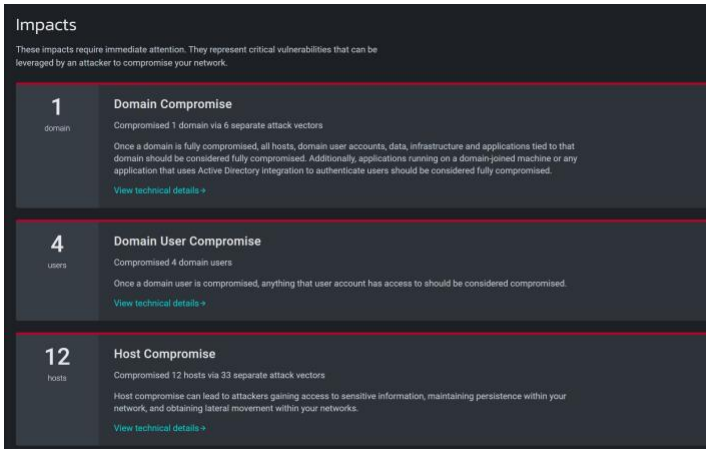
- Verify and improve your security controls – tools, processes, policies, and training.
- Continuously find + fix + verify what's exploitable.
- Adopt a Purple Team Culture, where red teams and blue teams work together to improve security posture.

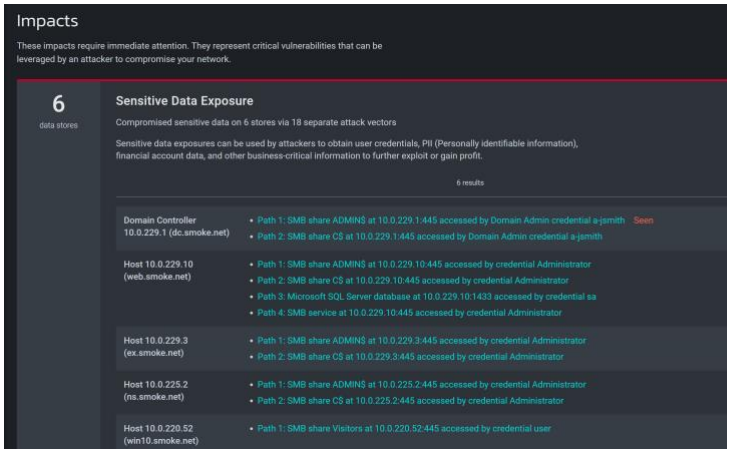
☐ ***Stay Ahead:***

- Look at your environment through the eyes of the attacker.
- Proactively identify and fix threat vectors before the bad guys can exploit them.
- Continuously assess your security posture, verify remediation, and report results.

CISOs, vulnerability managers, defensive teams, and IT Operators have limited resources and must prioritize efforts efficiently to begin to shift the economics of an attack back in their favor. This means contextually understanding vulnerabilities and their impacts for YOUR business.

As you move into a find, fix, verify cycle, adopting an agile security strategy, you'll begin to transition from the **Catch Up** phase, to the **Keep Up** phase. **NodeZero** provides the impact, proof, and the path within the **Impacts** tab of our portal. The goal is to get this tab to all zeros.

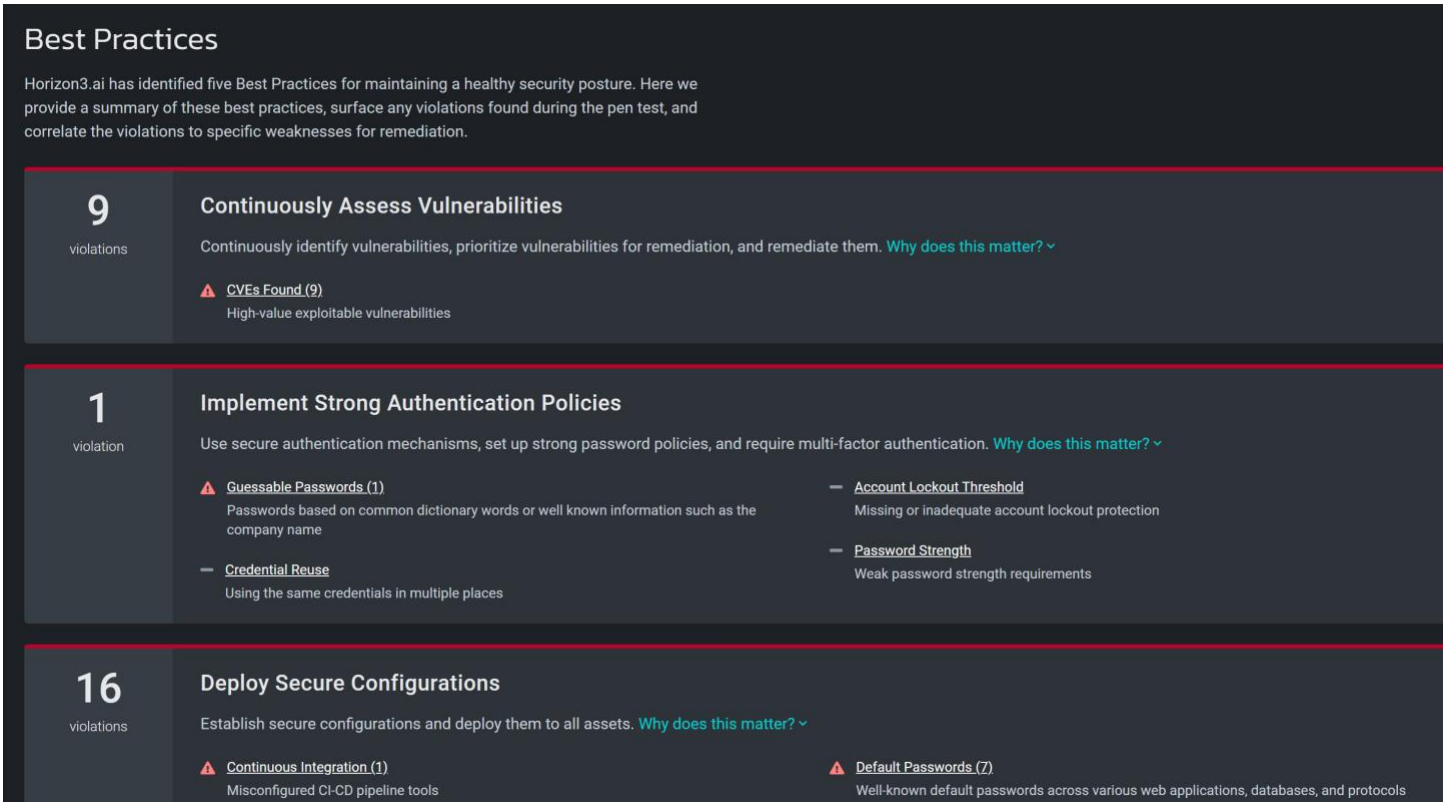




The **Stay Ahead** phase includes keeping the **Impacts** tab at all zeros, but also involves developing an understanding of where your policies, processes and procedures do or don't follow industry standards and best practices.

During a **NodeZero** operation, the system will come across indicators of how you apply or don't apply best practices. Though good indicators may not be definitive, **NodeZero** will surface the positive signs it came across within the scope of the operation. The information on the **Best Practices** tab will, however, highlight with certainty where we find blind spots. This information may include configuration management, password policies, web certificate management, access controls, authentication, etc.

With the new **Best Practices** tab, we analyze and enrich the **NodeZero** operation information and align it to categories of best practices to provide insight and inform written and technical policies. Where the impact tab provides an attacker's perspective on weaknesses with potential business impacts, the **Best Practices** tab gives a deeper look at where your security strategy is failing or succeeding.



With the publication of these new features, we are excited to give CISOs and security practitioners yet another set of insights that none of our competitors provide.

Catch Up, Keep Up and Stay Ahead with NodeZero and Horizon3.ai