



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.

Impacts
These impacts require immediate attention. They represent critical vulnerabilities that can be leveraged by an attacker to compromise your network.

- 1** Domain Compromise
Compromised 1 domain via 6 separate attack vectors
Once a domain is fully compromised, all hosts, domain user accounts, data, infrastructure and applications tied to that domain should be considered fully compromised. Additionally, applications running on a domain-joined machine or any application that uses Active Directory integration to authenticate users should be considered fully compromised.
[View technical details >](#)
- 4** Domain User Compromise
Compromised 4 domain users
Once a domain user is compromised, anything that user account has access to should be considered compromised.
[View technical details >](#)
- 12** Host Compromise
Compromised 12 hosts via 33 separate attack vectors
Host compromise can lead to attackers gaining access to sensitive information, maintaining persistence within your network, and obtaining lateral movement within your networks.
[View technical details >](#)

Impacts
These impacts require immediate attention. They represent critical vulnerabilities that can be leveraged by an attacker to compromise your network.

6 Sensitive Data Exposure
Compromised sensitive data on 6 stores via 18 separate attack vectors
Sensitive data exposures can be used by attackers to obtain user credentials, PII (Personally Identifiable Information), financial account data, and other business-critical information to further exploit or gain profit.

6 results

- Domain Controller (10.0.229.1 (dc.smoke.net))
 - Path 1: SMB share ADMIN\$ at 10.0.229.1:445 accessed by Domain Admin credential a.jamith [Seen](#)
 - Path 2: SMB share C\$ at 10.0.229.1:445 accessed by Domain Admin credential a.jamith
- Host 10.0.229.10 (web.smoke.net)
 - Path 1: SMB share ADMIN\$ at 10.0.229.10:445 accessed by credential Administrator
 - Path 2: SMB share C\$ at 10.0.229.10:445 accessed by credential Administrator
 - Path 3: Microsoft SQL Server database at 10.0.229.10:1433 accessed by credential sa
 - Path 4: SMB service at 10.0.229.10:445 accessed by credential Administrator
- Host 10.0.229.3 (ex.smoke.net)
 - Path 1: SMB share ADMIN\$ at 10.0.229.3:445 accessed by credential Administrator
 - Path 2: SMB share C\$ at 10.0.229.3:445 accessed by credential Administrator
- Host 10.0.225.2 (na.smoke.net)
 - Path 1: SMB share ADMIN\$ at 10.0.225.2:445 accessed by credential Administrator
 - Path 2: SMB share C\$ at 10.0.225.2:445 accessed by credential Administrator
- Host 10.0.220.52 (win10.smoke.net)
 - Path 1: SMB share Visitors at 10.0.220.52:445 accessed by credential user

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.

Best Practices

Horizon3.ai has identified five Best Practices for maintaining a healthy security posture. Here we provide a summary of these best practices, surface any violations found during the pen test, and correlate the violations to specific weaknesses for remediation.

9

violations

Continuously Assess Vulnerabilities

Continuously identify vulnerabilities, prioritize vulnerabilities for remediation, and remediate them. [Why does this matter? ▾](#)

- ▲ **CVEs Found (9)**
 High-value exploitable vulnerabilities

1

violations

Implement Strong Authentication Policies

Use secure authentication mechanisms, set up strong password policies, and require multi-factor authentication. [Why does this matter? ▾](#)

- ▲ **Guessable Passwords (1)**
 Passwords based on common dictionary words or well known information such as the company name
- **Credential Reuse**
 Using the same credentials in multiple places
- **Account Lockout Threshold**
 Missing or inadequate account lockout protection
- **Password Strength**
 Weak password strength requirements

16

violations

Deploy Secure Configurations

Establish secure configurations and deploy them to all assets. [Why does this matter? ▾](#)

- ▲ **Continuous Integration (1)**
 Misconfigured CI-CD pipeline tools
- ▲ **Default Passwords (7)**
 Well-known default passwords across various web applications, databases, and protocols

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

Best Practices

Catch Up, Keep Up, Stay Ahead Approach

