HORIZON3.ai
~~TRUST BUT~~ VERIFY

Sec4good

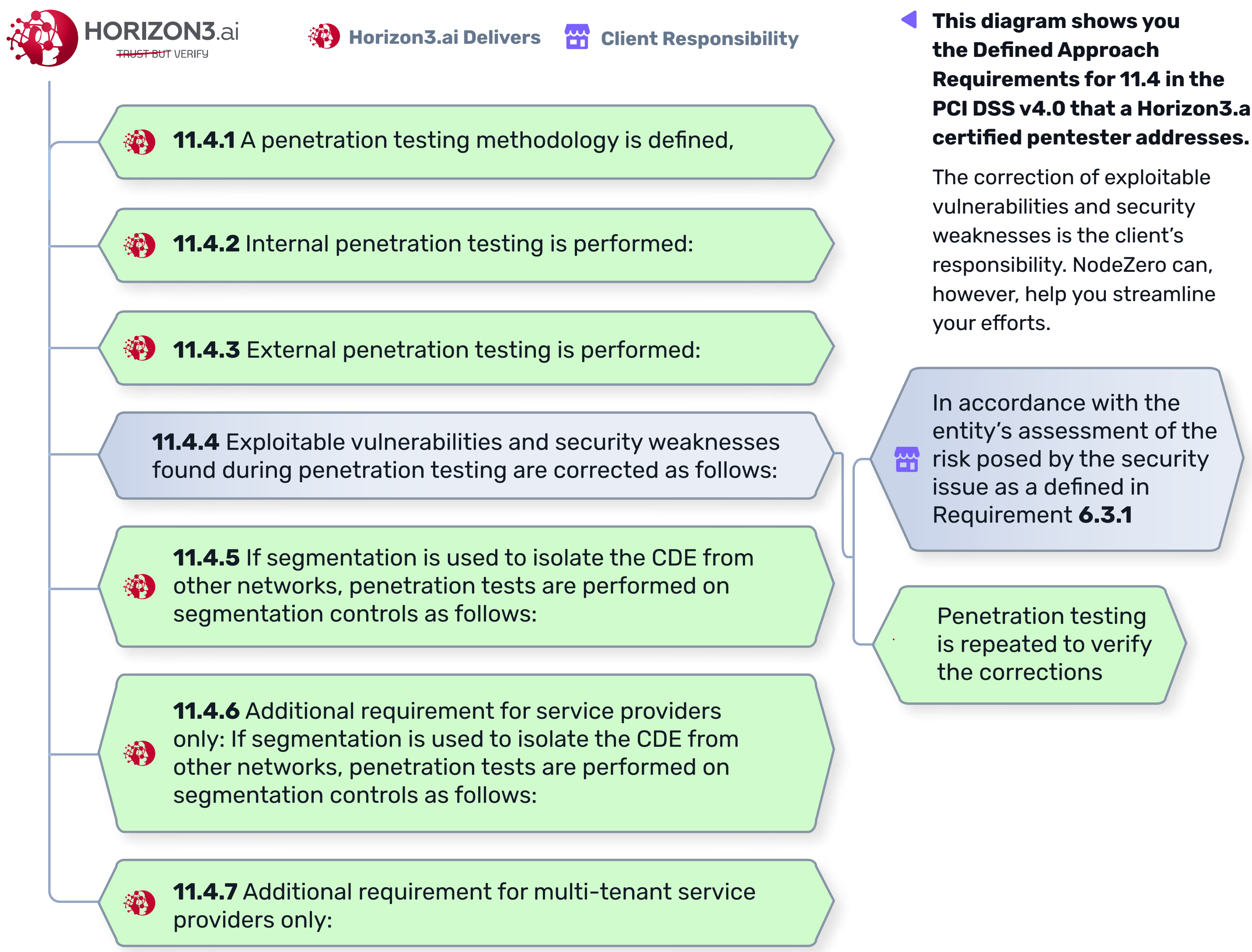
Horizon3.ai PCI 11.4 Pentesting Engagement

Fully satisfy your 11.4 pentesting requirements; improve your security posture

Horizon3.ai delivers sophisticated and timely penetration testing services tailored to fulfill the internal and external pentesting requirements of your cardholder data environment outlined by the Payment Card Industry Data Security Standard (PCI DSS) v4.0. Our offerings are executed with comprehensive coverage and meticulous attention to detail to fully address these stringent pentesting requirements.

Delivered by a World-Class Team with World-Class Tools

Our service is delivered by a world-class team of Offensive Security Certified Professional (OSCP) certified pentesters, equipped with the scale and depth of our Horizon3.ai NodeZero™ platform. This synergy between expert human skill sets and autonomous continuous testing delivered by NodeZero guarantees a thorough evaluation of your cardholder data environment (CDE). Following the pentest, you'll promptly receive a thorough and detailed report about the test findings that you can share with your auditor as essential evidence for your Report on Compliance (RoC) or submit with your PCI DSS Self-Assessment Questionnaires (SAQs).



HORIZON3.ai ~~TRUST BUT~~ VERIFY

Horizon3.ai Delivers

Client Responsibility

This diagram shows you the Defined Approach Requirements for 11.4 in the PCI DSS v4.0 that a Horizon3.ai certified pentester addresses.

The correction of exploitable vulnerabilities and security weaknesses is the client's responsibility. NodeZero can, however, help you streamline your efforts.

11.4.1 A penetration testing methodology is defined,

11.4.2 Internal penetration testing is performed:

11.4.3 External penetration testing is performed:

11.4.4 Exploitable vulnerabilities and security weaknesses found during penetration testing are corrected as follows:

In accordance with the entity's assessment of the risk posed by the security issue as a defined in Requirement **6.3.1**

Penetration testing is repeated to verify the corrections

11.4.5 If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows:

11.4.6 Additional requirement for service providers only: If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows:

11.4.7 Additional requirement for multi-tenant service providers only:

Better, faster, remediation, and targeted retesting with NodeZero

Your pentesting engagement with us extends beyond mere assessment; it includes access to a read-only version of NodeZero. An additional bundle option gives you the power of fully featured NodeZero for continuous security testing. With the bundle, you are able to independently conduct your own pentests and other key assessment operations.

The read-only version grants your organization 12 months of insightful access to your pentesting results and a comprehensive Fix Action report within the NodeZero portal. Our report not only meets Common Vulnerability Scoring System (CVSS) prioritization standards for vulnerabilities but surpasses them by tailoring priority levels and recommendations specifically for your organization's context. NodeZero intricately guides you through the most efficient remediation strategies, ensuring a streamlined approach to fortifying your cardholder data environment.

NodeZero is designed to inform and expedite your remediation efforts. The platform provides invaluable insights into the impact of the identified weaknesses in your Fix Action report. The platform view empowers you to delve into actionable fix actions for each vulnerability with ease. In addition, NodeZero shows you the fast path for addressing weaknesses at a systemic level. After your team has made the appropriate fixes, you can easily verify their effectiveness with the 1-click verify operation. This functionality performs targeted retesting, enabling your team to validate the success of your organization's efforts promptly. You can repeat 1-click verify tests as often as necessary over the length of your subscription.

Your ability to independently verify your remediations not only saves your team valuable time but also ensures readiness if retesting is required to fulfill 11.4.

Further, all PCI pentesting results and remediation activities conducted via our platform are securely stored for 12 months, adhering meticulously to PCI DSS requirement 11.4.1.

Receive Rapid Response Alerts for 12 Months

As an additional benefit, your subscription encompasses rapid response alerts from Horizon3.ai's accomplished Attack Team concerning potential zero-day and N-day vulnerabilities that could impact your environment, extending over 12 months. Numerous organizations opt to integrate their acquisition of the PCI 11.4 pentesting engagement with a bundled subscription to NodeZero for continuous security testing. This strategic approach not only surpasses mere "point-in-time" compliance but also alleviates the remediation burden for the forthcoming audit cycle.

Engagement Process Flow

Here is the standard flow for a Horizon3.ai PCI 11.4 pentesting engagement:

1. **Schedule the pentest.**

   A Horizon3.ai PCI 11.4 pentesting engagement can be scheduled at your convenience and will not interfere with your normal business activities.

2. **Meet with the OSCP expert to test your network and determine the scope of the cardholder data environment that will be thoroughly tested from both an internal and external perspective.**

   Horizon3.ai is both timely and thorough in delivery of this scoping.

3. **After the pentest, Horizon3.ai delivers you a thorough report and an accompanying Fix Action report.**

   By combining the skills of our experienced OSCP pentesters with the power and scale of NodeZero, the comprehensive and actionable results of your pentests can be delivered to you in a matter of days instead of the weeks that other pentesting services require.

   Your pentesting expert will talk you through both of these written reports and show you how the NodeZero platform can guide and expedite your remediation of any vulnerabilities that must be addressed in accordance with the PCI DSS v4.0.

4. **Your organization owns the responsibility for remediating vulnerabilities identified in the pentest in accordance with your organization's assessment of the risk posed by the security issues as defined by Requirement 6.3.1 in the PCI DSS v4.0.**

   You can use the prioritization in the NodeZero platform and your Fix Action Report to inform your remediation. It identifies weaknesses that meet the requirements for CVSS prioritization for vulnerabilities, but goes beyond that, contextualizing them for your organization. For example, when NodeZero chains together low CVSS score vulnerabilities to accomplish significant impacts, the CVSS score for that weakness is elevated to provide more accurate prioritization of how an attacker could exploit that weakness. NodeZero also provides guidance about how to most efficiently eliminate weaknesses.

5. **You can verify the effectiveness of your remediations with 1-click verify in the NodeZero platform and submit the 1-click verify report as evidence of the correction.**

   Static weaknesses identified by the pentest have a 1-click verify option for targeted testing so you can instantly evaluate whether your remediation was successful. When you have verified that the correction has been made, you can use the 1-Click Verify Report as evidence.

6. **Show the Horizon3.ai verification of pentesting and your corrections according to 11.4 to your auditor of choice as essential evidence for your annual Report on Compliance (RoC) or for your SAQs.**

   This engagement process also applies to your PCI DSS requirements for pentesting when there is any significant upgrade or change in your infrastructure or applications.

   Note: If you are required to conduct another pentest per 11.4.4, that is a separate engagement. You may retest with the pentester of your choice. There are advantages to re-engaging with Horizon3.ai because a retest done with a Horizon3.ai expert augmented by the NodeZero platform will be performed consistently with your original pentest, giving you a more accurate view of how you addressed the original vulnerabilities.

Meets Other Compliance Standards

Horizon3.ai penetration testing also meets the requirements of other standards including System and Organization Controls (SOC), Digital Operational Resilience Act (DORA), General Data Protection Regulation (GDPR), Center for Internet Security (CIS), National Institute of Standards and Technology (NIST), and Cybersecurity Maturity Model Certification (CMMC) standards.

Our cutting-edge testing methodologies and expert team ensure thorough examination of your systems, identifying vulnerabilities, and ensuring compliance with industry regulations. Trust Horizon3.ai to safeguard your data and infrastructure with precision and integrity.

HORIZON3.ai
~~TRUST BUT~~ VERIFY

Move to Continuous Security Testing

Compliance with the PCI DSS or other standards may be an annual exercise, but security is never a "one and done." You can bundle your purchase of the Horizon3.ai PCI pentesting engagement with a full subscription to the NodeZero platform. This allows you to:

- Continuously assess and improve your security posture with a number of operations beyond internal and external pentesting, such as AD password audit, the Phishing Impact test, and more.
- Proactively protect your cardholder data environment (CDE).
- Measure your progress over time.
- Reduce next year's compliance remediation through continuous security testing.

NodeZero is easy to use, safe for production, and scales to support your largest networks, empowering you to test a very broad scope and perform multiple operations concurrently.

Horizon3.ai Penetration Testing offers a comprehensive solution tailored to meet the rigorous requirements of GDPR, CIS, NIST, and CMMC standards. Our cutting-edge testing methodologies and expert team ensure thorough examination of your systems, identifying vulnerabilities and ensuring compliance with industry regulations. Trust Horizon3.ai to safeguard your data and infrastructure with precision and integrity.

Horizon3.ai was founded in 2019 by former industry and U.S. Special Ops cyber operators with the mission to help organizations see their networks through the eyes of the attacker and proactively fix problems that truly matter, improve the effectiveness of their security initiatives, and ensure that they are prepared to respond to real cyberattacks. Visit our website for a free trial and let our results do the talking. www.horizon3.ai

HORIZON3.ai

~~TRUST BUT~~ VERIFY