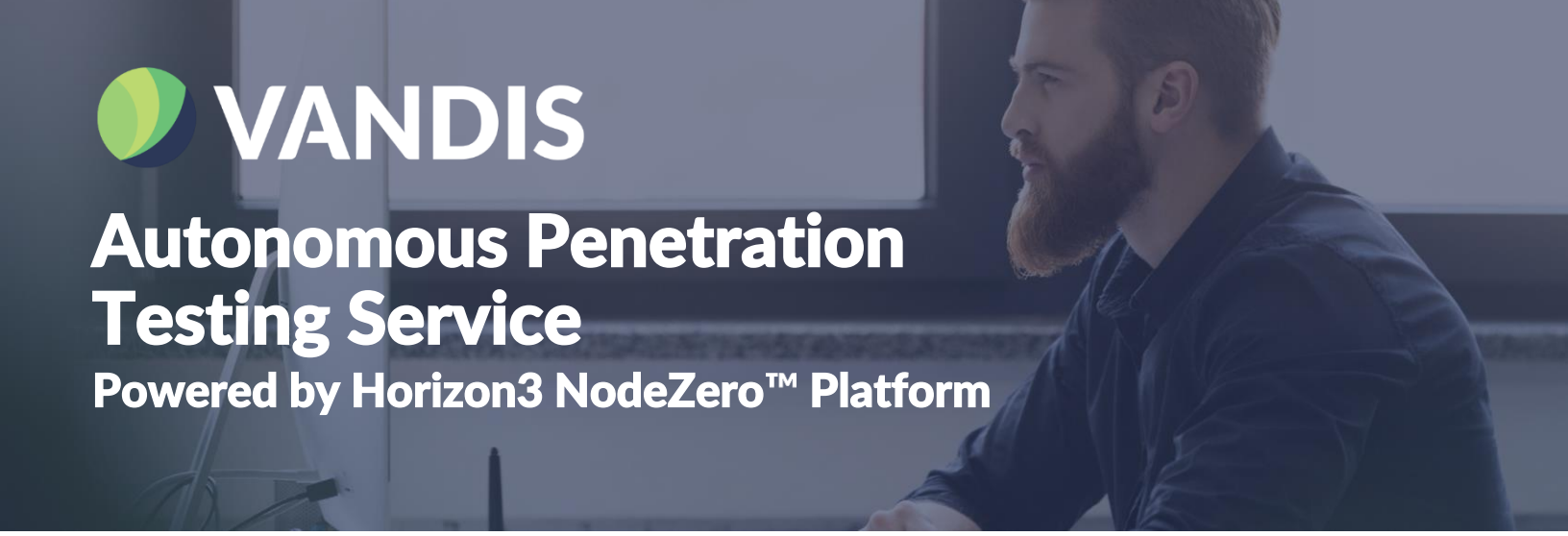


Autonomous Penetration Testing Service

Powered by Horizon3 NodeZero™ Platform

The Importance of Pentesting

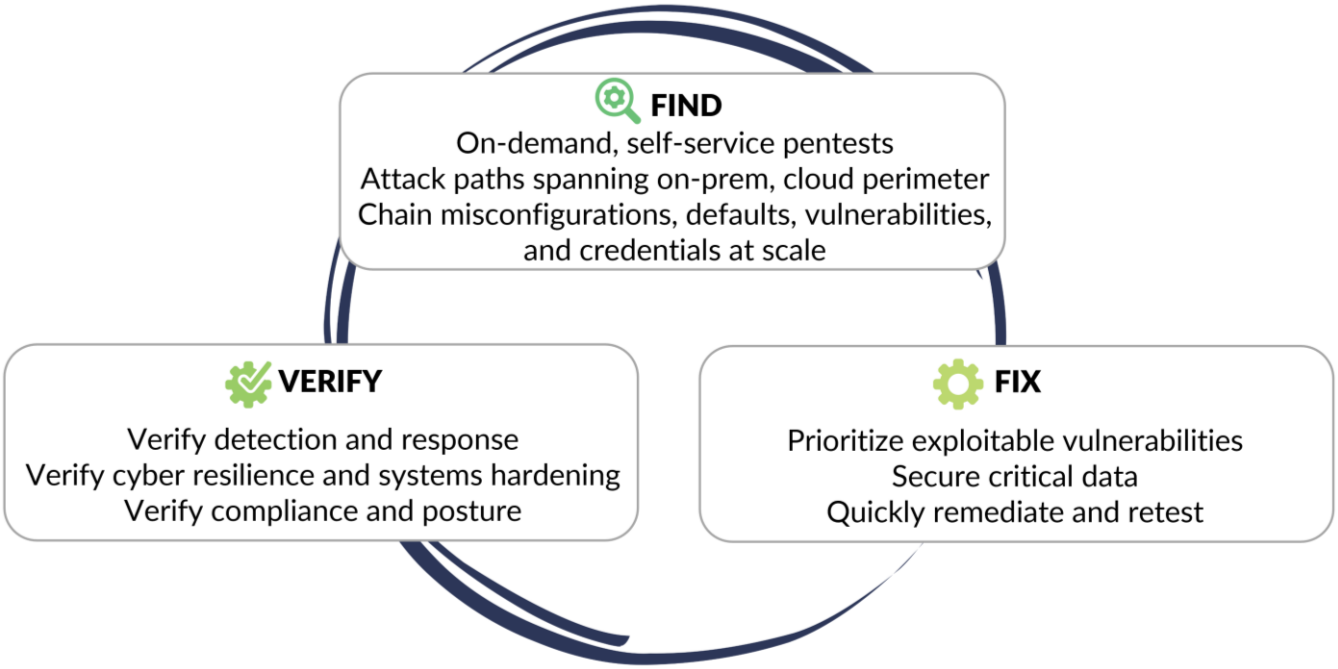
With the increasing risk of cyber attacks, it is important for organizations of all sizes to reduce their cybersecurity risk by finding the exploitable weaknesses in their network. Penetration testing brings value to organizations by identifying attack vectors and providing proof of exploitability. Pentesting can provide evidence that defensive controls are implemented effectively to focus remediation efforts on an organization's most critical weaknesses.

Autonomous Penetration Testing Service

Vandis' Autonomous Penetration Testing Service leverages the NodeZero™ platform to uncover the truly exploitable weakness in an organization's internal, external, and cloud infrastructures. The solution can help your organization continuously find, fix, and verify your exploitable attack surface. This on-demand, self-service SaaS platform is safe to run in production and requires no persistent or credentialed agents.

Vandis Service Highlights

- Flexible monthly, quarterly, and bi-annual service plans
- Access to the NodeZero™ platform to run pentests as often as you like
- Out-of-the-box and custom scans
- Reports, analysis, and prioritized recommendations
- Remediation services available as add-on package
- Packages starting as low as $10,000



© 2024 Vandis Inc. Vandis Confidential. All Trademarks are property of their respective owners. Vandis products and offerings, or those from our partners, are subject to change at any time without notice.

20240520

Service Inclusions

Flexible Service Plans: Choose a plan based on your IT Security team's needs. Select from either Monthly, Quarterly or Bi-annual plans for assessments to be run by the Vandis Managed Services team. Once a plan is selected, the Vandis Managed Services team will deploy and configure the NodeZero™ platform for your environment.

Direct Access: With this service, you also get direct access to the NodeZero™ platform. Run scans as often as you like. Use the platform to retest and verify the effectiveness of your remediation efforts.

Custom Pentests: The NodeZero™ platform comes with an out of the box internal IP and external IP test for your environment. Vandis Managed Services will provide up to two (2) additional custom tests that can be run either by Vandis Managed Services or by your IT security team. These pentests can be customized with variations in exploitation methods, credential verification, data exfiltration, and brute force attempts.

Expert Prioritized Recommendations: Based on your chosen package, you'll meet with Vandis security experts to review the result reports and analysis of the assessments. In addition, Vandis security experts will provide a summary of prioritized recommendations for remediation.

Starter Package: Think you can't afford a pentesting solution? Contact Us Today! Vandis offers a Starter Package to meet the needs of small-midsized businesses. **Packages starting at $10,000.**

REQUEST A DEMO

In this autonomous pentest attack path, NodeZero™ exploited two weaknesses – a Java JMX misconfiguration and SAM credential dumping – to achieve domain compromise.

Key Capabilities

- **Continuous Vulnerability Detection:** Immediate notification and reports for security team to begin remediation.
- **Efficient Remediation Verification:** Use 1-click verify to retest and verify effectiveness of remediation.
- **Prioritization of Vulnerabilities:** Rank based on severity, exploitability, and impact to the business.
- **Preemptively Respond to Emerging Threats:** Receive real-time threat alerts from the Rapid Response Attack Team to determine impact on your organization.
- **Proactive Threat Hunting:** Analyze patterns of identified vulnerabilities, look for anomalies, and preemptively hunt for potential threats.
- **Identify Data at Risk:** Simulate the behavior of an attacker and map exposed data back to data asset.
- **Determine the Blast Radius of a Compromised Credential:** Attack with a compromised credential to determine extent of access achieved.
- **Verify the Effectiveness of Security Tools (EDR, SIEM):** Monitor alerts and responses from your security tools to determine if it is time for tuning or an upgrade.

Why Vandis?

A comprehensive network and security strategy that spans your hybrid and premise environments is mission critical for your organization. Vandis' high-level engineering capabilities and close relationships with market leading and niche manufacturers allow us to make timely recommendations. With 40 years of experience, Vandis has the proven ability to navigate today's everchanging technology and business landscape and the resources and expertise to successfully manage projects on a regional, national, and global scale.

To learn more about Vandis' suite of assessments and health check services, contact us at info@vandis.com.

© 2024 Vandis Inc. Vandis Confidential. All Trademarks are property of their respective owners. Vandis products and offerings, or those from our partners, are subject to change at any time without notice.

VANDIS