

各 位

株式会社 JSOL

自律型ペネトレーションテストプラットフォーム「NodeZero®」の提供開始

～攻撃者が悪用できるセキュリティ上のリスクを継続的に検知・修正・検証～

株式会社 JSOL（以下、JSOL）は、Horizon 3 AI, Inc.（以下、Horizon3.ai）の自律型ペネトレーションテストプラットフォーム「NodeZero®」に関する国内唯一のマネージドセキュリティサービスプロバイダー（以下、MSSP）として、2026 年 6 月 1 日よりサービス提供を開始しました。NodeZero は、攻撃者視点の AI と自動化技術を活用し、企業の IT 環境に対する侵入経路や悪用され得る設定不備・認証情報のリスクを継続的に洗い出し、優先して対処すべき課題の特定と改善後の確認を支援する自律型ペネトレーションテストプラットフォームです。JSOL は MSSP として、日本企業が本サービスを分かりやすく、最大限に活用できるよう、導入から運用、評価結果の整理、改善に向けた対応検討までを一貫して支援します。加えて、当社の各種セキュリティソリューションおよびセキュリティ専門人材と連携し、経済産業省などが提示するセキュリティガイドラインへの準拠を支援する運用サービスを提供します。



【背景】

近年、AI の悪用・ランサムウェアをはじめ、サイバー攻撃は高度化・巧妙化しています。加えて、N-Day（開発元が提供している修正パッチについてユーザー側が適用していない期間を狙う攻撃）や Zero-Day（開発元が認識する前、または修正パッチを公開する前に悪用されるサイバー攻撃）といった脆弱性の悪用だけではなく、流出した認証情報や設定不備を悪用して正規利用者になりすます手口も増えています。従来の防御策だけでは実際にどの経路から侵入されたり被害拡大につながる恐れがあるのかを継続的に把握することが難しくなっています。例えば、脆弱性スキャナーが大量のアラートを発出しても「実際に悪用可能か」が不明なため、正しい優先順位が付けられません。また、手動による攻撃者侵入テストは、高コストかつ実施頻度が少なく、日々変化する IT 環境の継続的な保護には不十分です。

このため企業には、攻撃を受ける可能性を前提に、侵入の起点になり得る弱点と侵入後に被害が広がり得る経路の両方を継続的に評価し、優先順位を付けて対処していくことが求められています。さらに、認証情報の流出や設定不備といった実態に即したリスクを評価するには、ダークウェブやペーストサイトなどで実際に流通・公開されている情報も踏まえ、実害につながる観点で評価を行う必要があります。

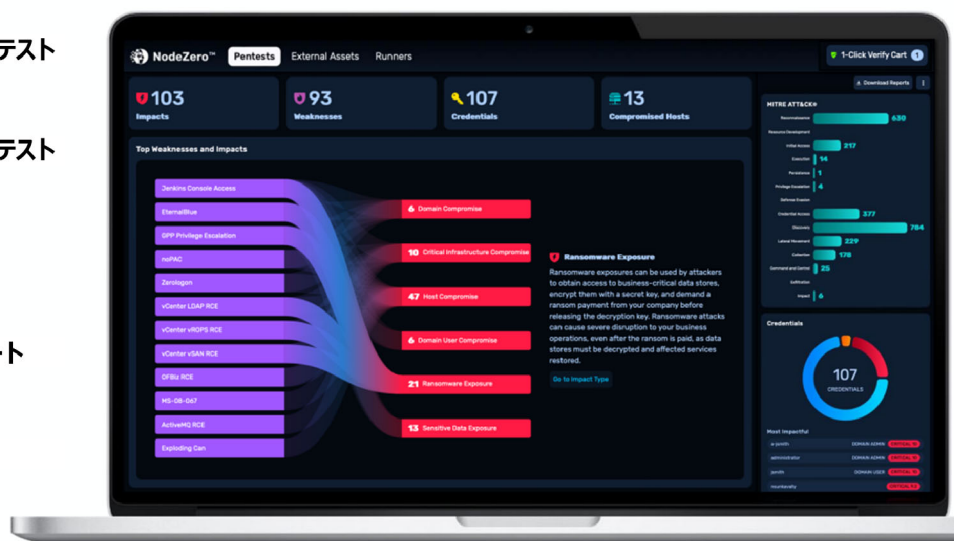
【NodeZero の主な特長】

NodeZero は、社内外の環境に存在する実際の攻撃者と同じ視点で、守るべき環境（オンプレミス/クラウド/ハイブリッド）へ攻撃者が侵入を試みるテスト「ペネトレーションテスト」を自律的かつ継続的に実施できるようにします。ペネトレーションテストを実行する専門家や複雑なスクリプトの準備などが不要で、防御対象の環境を設定するだけで簡単に、いつでもテストを実行することができます。さらに、ペネトレーションテストを実施した結果、実際に悪用される可能性のある攻撃ルートや被害の範囲をレポートの形式でまとめてくれます。

NodeZero にて実行できる主要なテストやシナリオは以下の通りです。

ペネトレーションテストの結果を表示する画面(イメージ)

- 内部ペネトレーションテスト
- 外部ペネトレーションテスト
- Rapid Response™
- フィッシング テンプレート
- ADパスワード監査



・社内外から悪用可能な攻撃経路を可視化

実際の攻撃で狙われやすい侵入経路をたどることで、権限昇格や横展開を含む被害拡大のシナリオを可視化することができます。

・Rapid Response™: N-Day／Zero-Day 両方の検証に対応

Horizon3.ai が提供する攻撃情報をもとに、N-Day／Zero-Day テストを迅速に実施し、重要なパッチ適用や対策の優先順位付けを支援します。

・フィッシングに伴う影響調査にも対応

疑似的なフィッシングで侵害された認証情報がどの範囲まで悪用されるかを確認し、影響の大きいリスクの把握に役立てます。（フィッシングのシミュレーションは別ソリューションを想定）

・Active Directory 監査による認証情報リスクの継続チェック

同一もしくは似ているパスワードが複数のアカウントで使い回しされていないかなど、認証情報に関わる不適切なプラクティスやリスクを監査し、継続的に確認することができます。

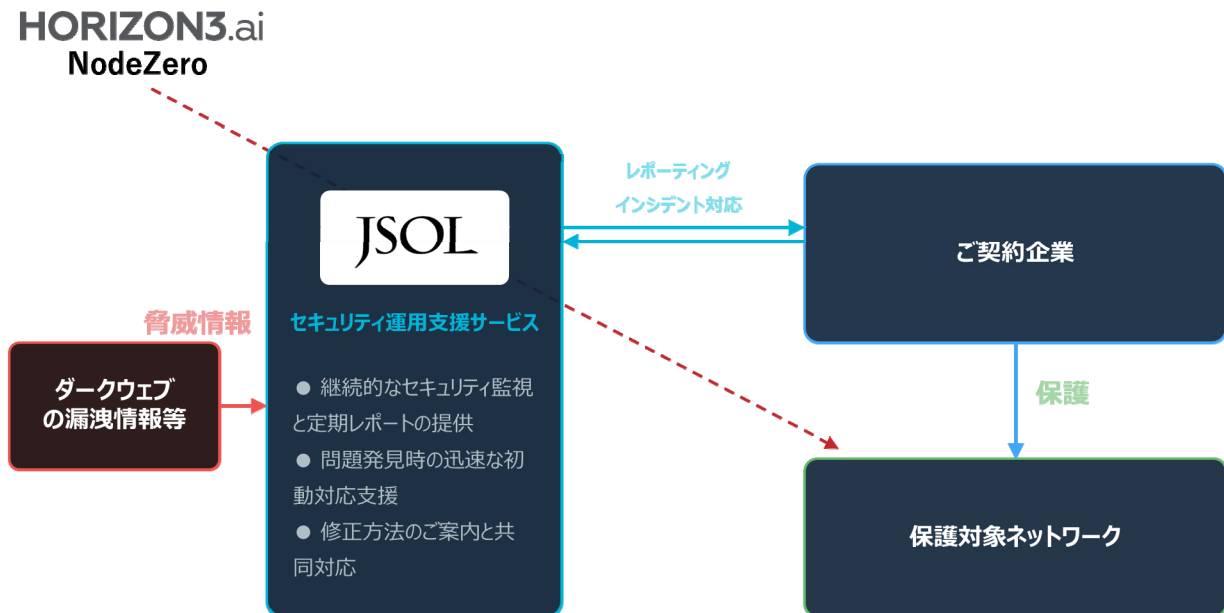
・NodeZero Tripwires™による侵入検知支援

攻撃者の活動を早期に察知するための仕組みを自動配置し、侵入の兆候を把握しやすくします。

これらにより、NodeZero は企業のセキュリティ運用において、リスクの発見、対策、改善確認を継続的に回すサイクルの実現を支援します。

【MSSP として JSOL が提供する付加価値】

JSOL は NodeZero の MSSP として、お客さまごとの環境に応じた導入支援、ペネトレーションテスト実施計画の調整、NodeZero ダッシュボードの評価結果の日本語での整理と報告、問題発見時の初動対応や修正方針の検討支援までを一体的に提供します。また、必要に応じて他のソリューションと組み合わせ、より実害につながり得る観点での評価や、セキュリティガイドライン準拠・監査対応の支援にもつなげます。



【Horizon3.ai からのエンドースメント】

(原文)

“We’re excited to partner with JSOL to help more organisations strengthen their security posture with Horizon3.ai. By giving customers an attacker’s-eye view of their environment, we help them identify exploitable risk, validate what matters most, and move faster on remediation. As organisations face a new wave of AI-powered attackers, this partnership will help customers stay ahead with a more proactive and realistic approach to security.”

About Horizon3.ai, Inc.

Horizon3.ai is the AI-native proactive security company redefining how organizations validate and strengthen their defenses. It is the company behind NodeZero®, the world’s best and most experienced AI hacker, trusted by 4 of the Fortune 10, global banks, and critical infrastructure operators. NodeZero enables organizations to proactively hack, fix, verify, and repeat testing on-demand, resulting in stronger defenses and measurable improvements in cyber resilience.

Horizon3.ai was founded by former U.S. Special Operations members and industry experts.

<https://horizon3.ai/>

(日本語訳)

「JSOL とのパートナーシップを大変嬉しく思います。本提携により、より多くの企業が Horizon3.ai を活用してセキュリティ態勢を強化できるようになります。

私たちは、攻撃者の視点からお客さまの環境を可視化することで、実際に悪用され得るリスクを特定し、優先的に対応すべき課題を検証し、迅速な対策実行を支援します。

AI を活用した攻撃が新たな脅威として拡大する中、本パートナーシップは、よりプロアクティブかつ現実的なセキュリティアプローチによって、お客さまが脅威に先手を打つことを可能にします。」

Horizon3.ai, Inc.について

Horizon3.ai は、AI ネイティブなプロアクティブセキュリティ企業であり、企業が自らの防御態勢を検証・強化する方法を再定義しています。

同社は、世界最高水準かつ豊富な実績を持つ AI ハッカー「NodeZero®」を提供しており、Fortune 10 企業（上位 10 社）のうち 4 社をはじめ、グローバル銀行や重要インフラ事業者から信頼を得ています。

NodeZero は、組織がオンデマンドで継続的に「攻撃（ハック）→修正→検証」を実施できる環境を提供し、防御力の強化とサイバーレジリエンスの向上を実現します。

Horizon3.ai は、米国特殊作戦部隊の出身者および業界の専門家により設立されました。

<https://horizon3.ai/>

■関連サイト

https://promotion.jsol.co.jp/SecAIOps/security-network/Node_Zero/index.html

■株式会社 JSOL

（本社：東京都千代田区、代表取締役社長：永井 健志）

<https://www.jsol.co.jp/>

株式会社 JSOL は、株式会社 NTT データと株式会社日本総合研究所が出資するシステムコンサルティング・ソリューションインテグレーターです。

2006 年の設立以来、製造、流通サービス、金融、公共分野で培った豊富な業務ノウハウとシステム開発力、エンジニアリングサイエンス分野における先進的な解析技術に強みを持ち、お客さまの価値向上に貢献しています。

※本リリースに記載されている内容は予告無く変更することがあります。

※本リリースに記載されている製品名、会社名は各社の商標または登録商標です。

【お問い合わせ先】

一般のお客さま

株式会社 JSOL サイバーセキュリティ&インテリジェント・オペレーション事業本部

E-Mail: hg_security_solutions_info@s1.jsol.co.jp

報道関係者さま

株式会社 JSOL 経営企画本部 広報部

E-Mail: webinfo@jsol.co.jp

JSOL CORPORATION