HORIZON3.ai

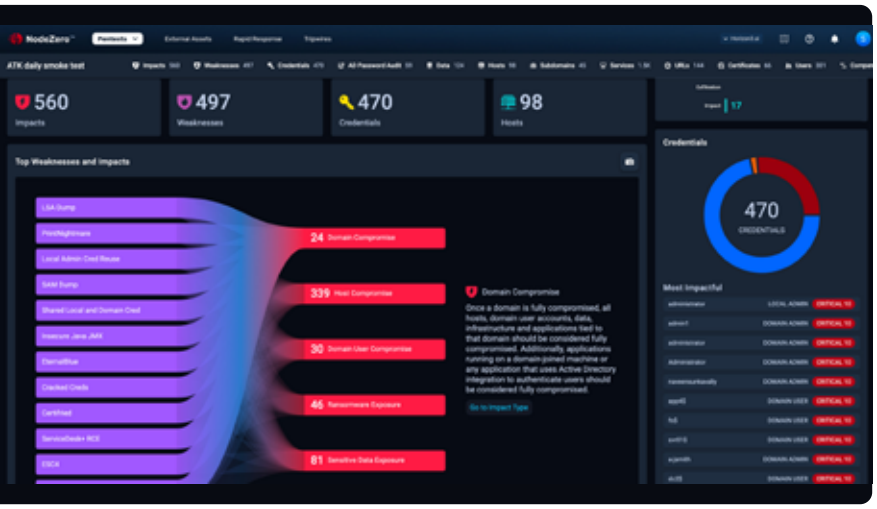
~~TRUST BUT~~ VERIFY

NodeZero

Trouver, réparer et vérifier en continu les faiblesses de votre cybersécurité

La plateforme NodeZero™ permet à l'entreprise de réduire les risques de sécurité en trouvant de manière autonome les faiblesses exploitables dans le réseau, en fournissant des conseils détaillés sur la manière de les prioriser et de les corriger, et en aidant à vérifier immédiatement que les correctifs sont efficaces.

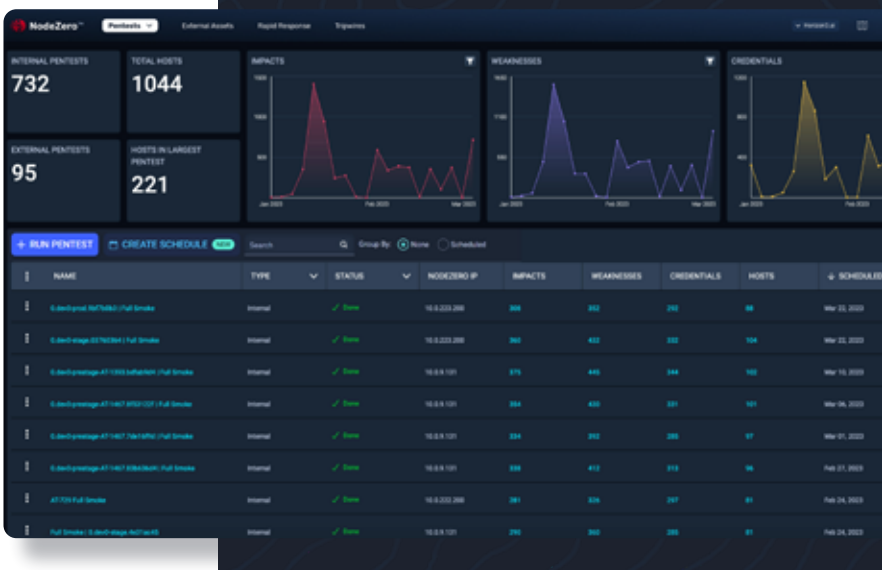
Découvrez les angles morts de votre posture de sécurité, au-delà des vulnérabilités connues et correctives, telles que les identifiants facilement compromis, les données exposées, les mauvaises configurations, les contrôles de sécurité insuffisants et les politiques faibles.



▲ NodeZero vous aide à comprendre les faiblesses qui conduisent à des impacts critiques, afin que vous sachiez exactement quoi corriger pour perturber la kill chain.

Navigue sur votre réseau, suit une chaine de faiblesses comme le ferait un attaquant, puis les exploite de manière sûre.

Planifiez et exécutez autant de tests d'intrusion que souhaité contre votre infrastructure numérique. Exécutez plusieurs tests d'intrusion en même temps.



▲ Le tableau de bord priorise les risques et aide à surveiller les progrès au fil du temps.

Améliorez les compétences de votre équipe IT, quel que soit leur niveau d'expertise. Vous pouvez configurer et démarrer votre premier NodeZero en quelques minutes.

Effectuez des tests illimités :

- infrastructure on-premise
- infrastructure Cloud
- infrastructure IAM
- infrastructure Kubernetes
- infrastructure de données
- infrastructure virtuelle
- actifs ouverts au public

La vue en temps réel donne une visibilité sur les exploits de NodeZero au fur et à mesure de leur exécution. Vous pouvez voir la preuve, le chemin et l'impact de chaque faiblesse identifiée.

Les rapports sont conçus pour aider à répondre aux exigences d'audit internes et externes. Ils incluent un résumé exécutif, des rapports de test d'intrusion, d'actions de correction, de segmentation et plus encore.

NodeZero exécute de manière autonome ces opérations pour évaluer et valider votre posture de sécurité :

Pentesting interne

Déployable sur site, hybride, k8s ou dans le cloud. Adoptez la perspective d'un attaquant avec un accès initial interne à votre infrastructure et prioriser les impacts prouvés nuisibles à la sécurité de l'organisation, avec des conseils détaillés de remédiation.

Pentesting externe

Lancé depuis l'environnement cloud de Horizon3.ai sans configuration supplémentaire, les tests d'intrusion externes évaluent rapidement et avec précision votre posture de sécurité du point de vue d'un attaquant tentant de franchir votre périmètre.

Réponse Rapide et Test N-Day

Ce service unique fournit des renseignements en temps réel sur les menaces émergentes, vous permettant d'utiliser ces renseignements dans le centre de Réponse Rapide pour atténuer les menaces avant qu'elles ne soient exploitées dans la réalité.

Test d'Impact de Phishing

Découvrez les dégâts qu'un attaquant peut causer avec des identifiants phishés dans votre environnement. NodeZero aide à mesurer et comprendre l'impact prouvé d'une escroquerie par phishing et recommande des contrôles pour atténuer le risque.

Pentesting Cloud

NodeZero se concentre sur la surface d'attaque des identités, se déployant pour identifier les faiblesses ou les mauvaises configurations IAM qui conduisent à l'escalade de privilèges, à la surexposition des actifs cloud, et aux vulnérabilités que des initiés malveillants ou des attaquants externes pourraient exploiter.

Audit des Mots de Passe AD

Les attaquants ne piratent pas, ils se connectent. Les identifiants compromis sous-tendent un pourcentage élevé de cyberattaques. Vérifiez continuellement l'efficacité de vos politiques d'identifiants pour vous assurer de ne pas laisser un tapis de bienvenue pour les mauvais acteurs.

NodeZero Tripwires

Lors d'un test d'intrusion, NodeZero place stratégiquement des leurres—comme des fichiers et des identifiants fictifs—basés sur les chemins d'attaque exploitables qu'il découvre. Si un acteur malveillant interagit avec un fil d'alerte, une alerte immédiate est envoyée de NodeZero aux équipes de sécurité.

Schedule a demo now.

https://www.horizon3.ai/demo

MIEL

Appelez MIEL
au 01 60 19 34 52
www.miel.fr/horizon3

Continuously improve your cyber resilience.

HORIZON3.ai
~~TRUST~~ BUT VERIFY