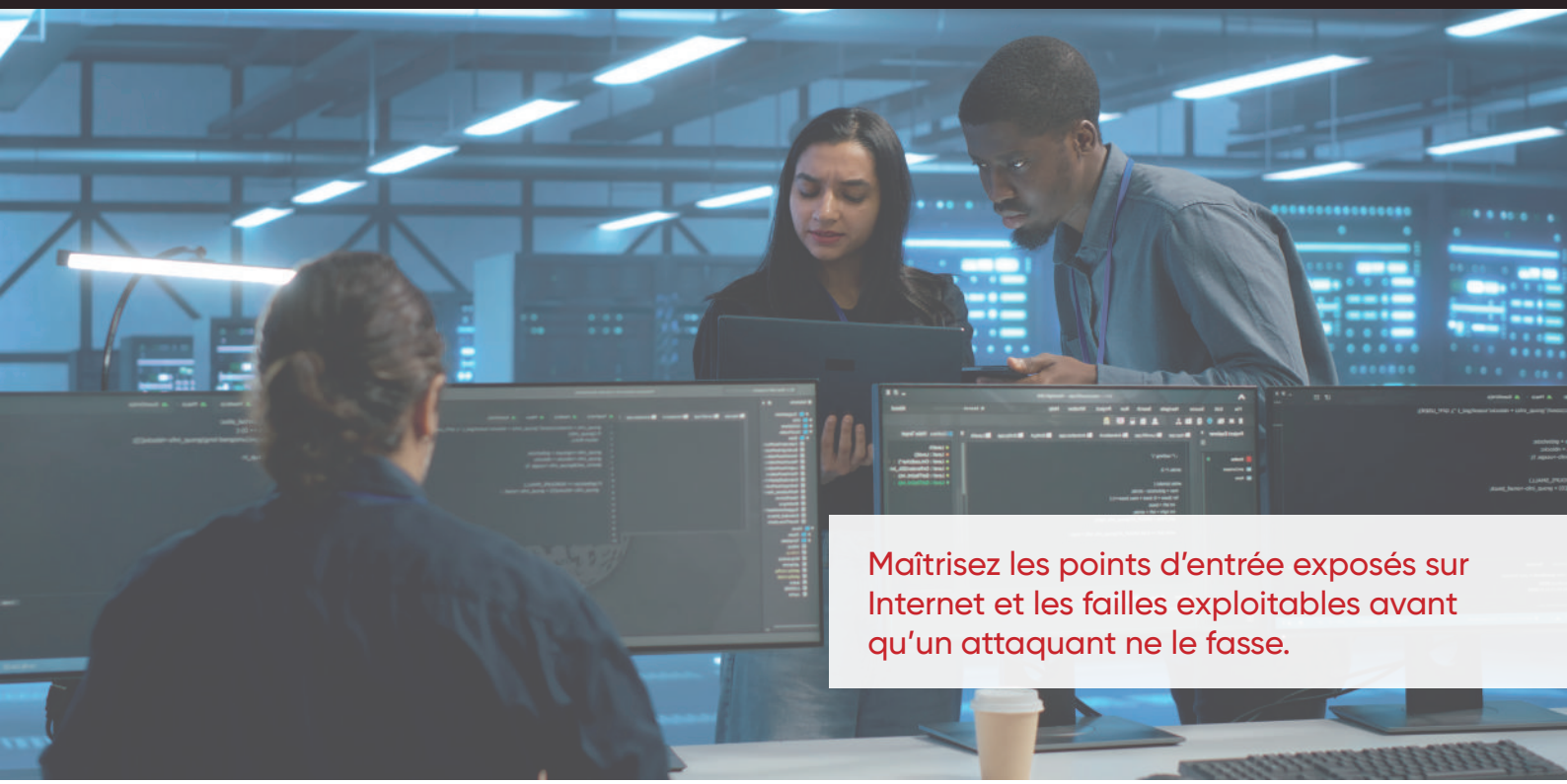
VIVALTEK | PUBLIC IP CONTROL



Maîtrisez les points d'entrée exposés sur Internet et les failles exploitables avant qu'un attaquant ne le fasse.

INTRODUCTION

Une faille exploitée engendre des risques pour votre activité ainsi qu'une atteinte à votre image de marque. Les cyberattaquants s'appuient sur diverses sources pour identifier les vulnérabilités exploitables afin d'atteindre leurs objectifs. C'est pourquoi un scan d'IP publique est essentiel : il permet de détecter les ports ouverts, les services exposés, les vulnérabilités connues et les configurations à risque, réduisant ainsi les opportunités pour les attaquants. Notre audit vous aide à reprendre le contrôle : il **sécurise vos systèmes, protège vos données et renforce la confiance de vos clients.**

Protégez vos informations, gagnez en sérénité et assurez votre conformité… avant qu'un incident ne vous y contraigne.

OBJECTIFS

Obtenir une visibilité précise de la surface d'exposition sur Internet en identifiant les services accessibles, les ports ouverts ainsi que les vulnérabilités connues (CVE[1]) exploitables par un attaquant.

- **Démontrer la maturité et la proactivité de l'entreprise**
- **Cartographier la surface d'attaque**
- **Réduire les risques d'intrusion**
- **Renforcer la confiance des clients**
- **Eviter les coûts financiers qu'impliquerait un incident.**

LES CHIFFRES CLÉS*

53 %

des entreprises françaises, en 2023, ont été victimes d'une cyberattaques, contre 48% en 2022.

14 720 €

c'est l'estimation du coût moyen d'une attaque.

280 000

c'est le nombre de demandes d'assistance reçues par Cybermalveillance.gouv.fr en 2023.

+17 %

de hausse du nombre de cyberattaques chez les collectivités et 13% chez les particuliers.

**Toutes les sources sont disponibles sur notre site internet, dans la fiche produit correspondante.*

CONTACTEZ NOTRE EXPERT 02 52 61 46 75 | contact@vivaltek.com

Comment fonctionne Public IP Control ?

Ce module commence par **identifier les adresses IP publiques** accessibles depuis Internet pour ensuite les analyser. Il **génère un rapport** avec le détail des ports, des services exposés, la liste des vulnérabilités (avec leurs CVSS) et donne une **évaluation globale**.

Sur quoi s'appuie Public IP Control ?

- **Ports ouverts et services actifs :** détection des ports ouverts (22, 80, 443, 445, etc.) et des des services actifs associés (Apache, OpenSSH, Samba, MySQL...),
- **Bases publiques de vulnérabilités :** une fois les versions logicielles identifiées, nos solutions s'appuient sur des bases de données publiques (CVE, NVD[2], exploit-db),
- **Vérifications globales :** identification de la présence de certificats SSL valides, analyse des headers HTTP de sécurité, et détection de la présence éventuelle d'un pare-feu ou d'un mécanisme de filtrage applicatif.

Pourquoi effectuer une simulation Public IP Control ?

En auditant votre IP, ce module **détermine votre surface d'attaque réelle** et identifie les ports et services accessibles utilisés par vos applications (comme Apache, SSH, SMTP).

Il **détecte en continu les failles ou mauvaises configurations potentielles**, qu'il s'agisse de ports ouverts vulnérables, de services obsolètes ou d'erreurs de configuration. Cette vigilance **aide les structures à protéger** efficacement leur réputation et leur activité, tout en répondant aux exigences réglementaires comme le RGPD, la norme ISO 27001[3] ou la directive NIS2.

Simulation avec Public IP Control :

Le scan de domaine **révèle la surface d'attaque réelle d'une entreprise en identifiant failles, services exposés et vulnérabilités**. Il permet d'anticiper les risques d'intrusion, de garantir la continuité d'activité et de répondre aux exigences de conformité. **C'est une démarche stratégique de prévention.**

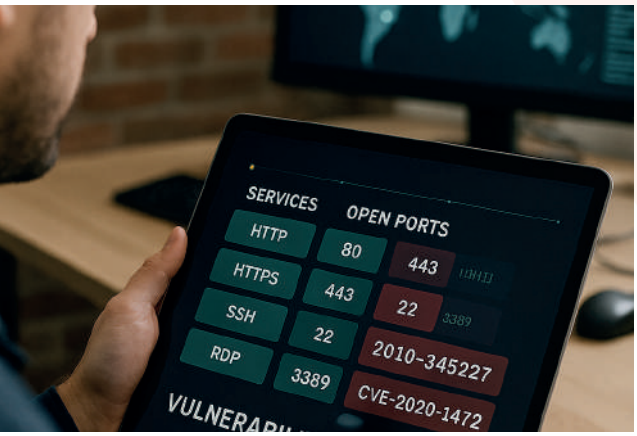
Sur quelle fréquence évaluer votre système Public IP Control ?

L'exposition de vos systèmes à Internet évolue en permanence : déploiements, mises à jour, erreurs humaines ou nouvelles vulnérabilités critiques peuvent rendre votre infrastructure visible et vulnérable en un instant. C'est pourquoi une **analyse régulière** de vos domaines et IP publiques est devenue une exigence incontournable pour toute organisation souhaitant **se prémunir durablement contre les cybermenaces.**

Grâce à cette fréquence, vous bénéficiez :

- D'un **suivi régulier** de votre surface d'attaque externe,
- D'une **détection rapide** des ouvertures non maîtrisées (ports, services exposés, sous-domaines oubliés…),
- Et d'un **pilotage proactif** de vos actions de remédiation.

Vous répondez ainsi aux exigences des normes de sécurité **(NIS2, ISO 27001, DORA, RGPD)** et démontrez une gouvernance active de vos actifs numériques exposés.



Notre objectif : Obtenir une visibilité précise de la surface d'exposition sur Internet en identifiant les services accessibles, les ports ouverts ainsi que les vulnérabilités connues (CVE) exploitables par un attaquant.

Lexique

[1]**CVE (Common Vulnerabilities and Exposures) :** Ce terme est un identifiant unique donné à une faille de sécurité informatique connue, pour la répertorier et la partager publiquement. Elle permet aux entreprises et aux experts de connaître, suivre et corriger plus facilement les vulnérabilités dans les logiciels et systèmes.

[2]**NVD (National Vulnerability Database) :** C'est la base de données officielle des vulnérabilités gérée par le gouvernement américain via le NIST (National Institute of Standards and Technology).

[3]**ISO27001 :** Norme internationale qui définit les exigences pour mettre en place un système de gestion de la sécurité de l'information afin de protéger les données sensibles, réduire les risques et garantir la confidentialité, l'intégrité et la disponibilité des informations.

Consultez notre lexique complet à l'adresse suivante : https://vivaltek.com/lexique-complet

VIVALTEK
2, Impasse Johannes Gutenberg, Z.A Les Acacias III 85430 La Boissière des Landes
02 52 61 46 75 | contact@vivaltek.com