VIVALTEK | PUBLIC DOMAINE CONTROL

Maîtrisez la surface d'attaque de vos domaines et identifiez les données sensibles exposées sur Internet ou le Dark Web.

INTRODUCTION

Une faille exploitée, c'est un risque pour votre activité et une image de marque entachée.

Nous révélons l'exposition réelle de votre domaine sur Internet et le Dark Web, en **identifiant les données sensibles déjà compromises**. Nos solutions détectent les vulnérabilités exploitables afin de réduire efficacement votre surface d'attaque.

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

OBJECTIFS

Analyser l'exposition publique d'un domaine ou d'un site internet afin de détecter les données sensibles accessibles sur Internet ou le Dark Web.

- **Evaluer les risques liés aux informations sensibles**
- **Anticiper des attaques ciblées**
- **Identifier des failles exploitables**
- **Valoriser votre image et préserver votre réputation**
- **Protéger vos données**

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 en 2023.

**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 Domaine Control ?

Le module scan d'un domaine externe permet d'**analyser les vulnérabilités** associées à un domaine ou à un site internet.

Elle réalise plusieurs vérifications, notamment : la **cartographie des sous-domaines actifs, l'identification des vulnérabilités** et des **CVE[1] associées**, ainsi que le contrôle de la conformité RGPD[2] du site analysé.

Sur quoi s'appuie Public Domaine Control ?

- **Cartographie DNS et des sous-domaines :** identification du périmètre d'exposition du domaine sur internet,
- **Scan des ports et services exposés :** détection des ports accessibles publiquement et identification de ceux pouvant représenter une faille de sécurité,
- **Analyse des vulnérabilités connues (CVE) :** recherche des failles critiques fréquemment exploitées par les attaquants,
- **Contrôle des bonnes pratiques et configurations:** vérification de la présence d'un certificat SSL, de la sécurisation des pages d'administration, et de la configuration générale du site pouvant faciliter une intrusion,
- **Audit CMS et conformité RGPD :** évaluation de la sécurité du CMS utilisé, détection de failles connues, et vérification de la conformité du site aux exigences du RGPD,
- **Vérification de l'environnement d'hébergement :** analyse de la localisation des données, des mesures de sécurité mises en place par l'hébergeur, et de la gestion du risque via un plan de reprise d'activité (PRA) ou de continuité (PCA).

Pourquoi effectuer une simulation Public Domaine Control ?

1. **Réaliser un scan de domaine permet de visualiser la surface d'attaque externe réelle** d'une entreprise, exactement comme la percevrait un attaquant.

2. **Identifier les services exposés**, les ports ouverts, les vulnérabilités connues (CVE) et les mauvaises configurations susceptibles d'être exploitées.

3. **Détecter ces failles** en amont réduit le risque d'intrusion, de vol de données ou d'interruption de service, tout en préservant la continuité d'activité et l'image de marque.

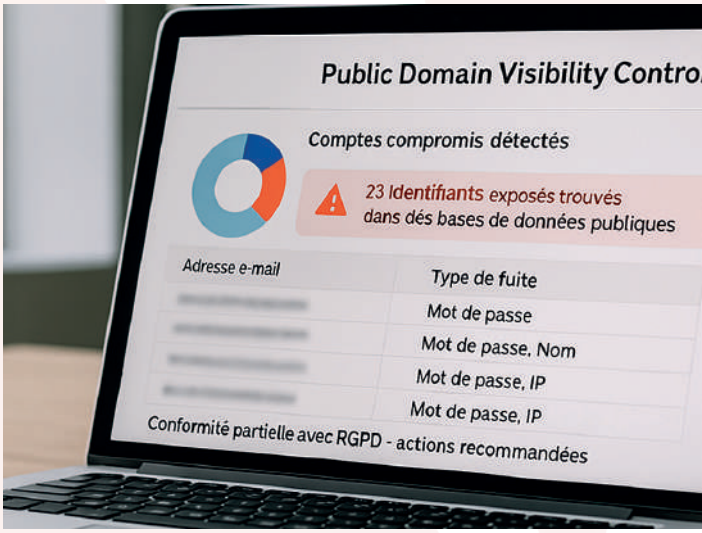
4. **Respecter la conformité : RGPD, ISO 27001, directive NIS2** ou encore les exigences des assureurs qui imposent une connaissance précise et une documentation régulière des actifs exposés et de leur niveau de sécurité.

5. **Scanner son domaine**, c'est choisir l'**anticipation plutôt que la réaction**, en investissant dans la prévention plutôt que dans la gestion de crise, souvent bien plus coûteuse.

Simulation avec Public Domaine 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 Domaine Control ?

L'exposition de votre domaine sur 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[3], RGPD)** et démontrez une gouvernance active de vos actifs numériques exposés.

Ce module évalue les risques, identifie les vulnérabilités exploitables et analyse l'exposition publique d'un site afin de détecter les données sensibles accessibles sur Internet ou le Dark Web.

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]RGPD (Règlement Général sur la Protection des Données) : Le RGPD est une loi européenne qui oblige les entreprises à protéger les données personnelles de leurs clients, utilisateurs ou employés, et à être transparentes sur la façon dont ces données sont collectées et utilisées.

[3]DORA : Réglementation européenne qui impose aux entreprises du secteur financier de renforcer leur résilience face aux cyber-risques.

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