

OTOCYON

L'audit cyber terrain pour savoir ce que votre réseau expose réellement

Une solution Isatis Concept



Beaucoup d'entreprises ignorent quels équipements, services ou accès sont réellement visibles sur leur réseau.

OTOCYON apporte rapidement une vision claire des risques techniques exposés, avec un rapport priorisé et des actions concrètes à engager.



Pourquoi faire un audit OTOCYON ?

- Identifier les équipements visibles
- Repérer les services et ports exposés
- Repérer les signaux de vulnérabilité
- Obtenir une vision claire et actionnable
- Prioriser les actions de sécurisation



Ce que nous faisons

Lors de l'intervention, **OTOCYON** est branché sur un point réseau autorisé. L'audit permet de découvrir les équipements visibles, d'identifier les services exposés, de rapprocher les résultats avec les vulnérabilités connues et de produire une cartographie simplifiée de votre SI.



Ce que vous recevez

- Rapport clair et compréhensible
- Cartographie simplifiée du SI visible
- Risques priorisés
- Recommandations concrètes
- Proposition d'accompagnement

Offre de lancement

À partir de

990 €

HT / site audité

Audit sur site, analyse et rapport confidentiel inclus



Ce n'est pas

OTOCYON n'est pas un test d'intrusion offensif.

Il s'agit d'un diagnostic cyber terrain, non intrusif, sans exploitation de faille, conçu pour donner rapidement une vision claire des risques visibles et des actions prioritaires.

Tarif valable jusqu'à **70 km** autour de Dijon.
Au-delà, forfait déplacement sur devis.



www.isatis-concept.fr

Vous avez un doute sur votre exposition réseau ?

Parlons-en.

contact@isatis-concept.fr

03 73 27 57 02



**Isatis
Concept**

OTOCYON

L'audit cyber terrain pour savoir ce que votre réseau expose réellement

Une solution Isatis Concept



Comment se déroule l'audit ?



Préparation

Nous validons avec vous le site à auditer, le point d'accès au réseau et les contraintes techniques.



Intervention sur site

OTOCYON est branché. L'analyse est non intrusive et n'interrompt pas votre activité.



Analyse

Les équipements, services exposés et signaux de vulnérabilité sont analysés et priorisés.



Restitution

Vous recevez un rapport clair, une cartographie simplifiée et des recommandations concrètes.

Ce que l'audit permet de voir

- Les équipements visibles sur le réseau
- Les services et ports exposés
- Les technologies ou versions détectables
- Les signaux de vulnérabilité connus
- Une cartographie simplifiée du SI visible
- Les priorités de sécurisation

Vos questions fréquentes

L'audit va-t-il interrompre mon activité ?

Non. L'approche est non intrusive et conçue pour ne pas perturber vos systèmes.

Avez-vous accès à nos données métier ?

Non. L'objectif est d'observer les équipements et services visibles, pas de consulter vos fichiers.

Combien de temps dure l'intervention ?

La durée dépend du site mais l'offre est pensée pour rester simple et rapide.

Que se passe-t-il après le rapport ?

Vous pouvez traiter les recommandations en interne, avec votre prestataire habituel, ou demander un accompagnement à Isatis Concept.

Les limites de l'audit

OTOCYON ne remplace pas un audit complet de cybersécurité, un test d'intrusion ou une analyse exhaustive du système d'information.

L'audit de base est limité à un maximum de 500 périphériques.



www.isatis-concept.fr

Vous avez un doute sur votre exposition réseau ?

Parlons-en.

contact@isatis-concept.fr

03 73 27 57 02

