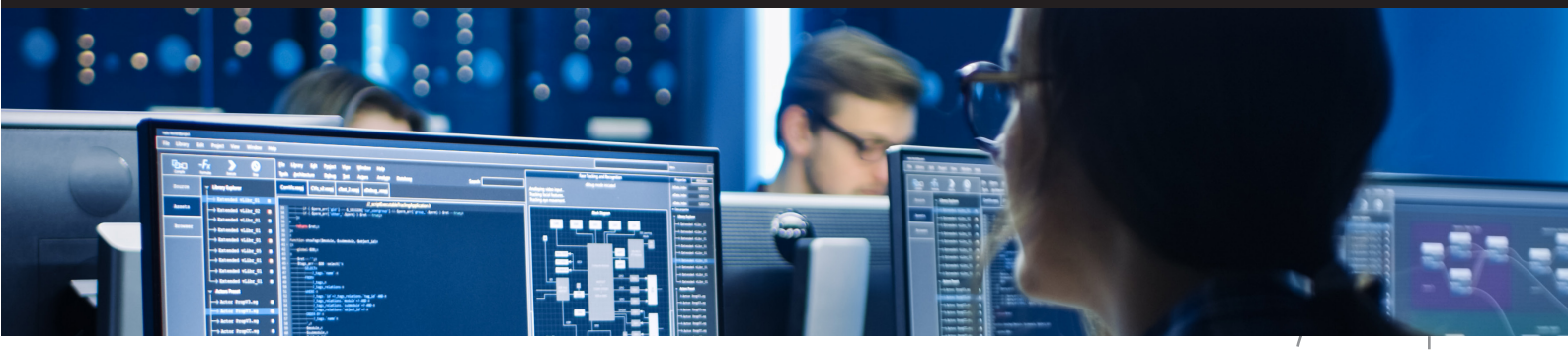
Orange Cyberdefense



Cyber Diagnostic

Déterminer votre réelle surface d'exposition aux risques cyber

Quelques chiffres

75%

des attaques se font sur les sociétés de taille moyenne.

Source : Security Navigator 2023

60%

des PME mettent la clé sous la porte dans les six mois suivant une cyberattaque.

Source : Security Navigator 2023

25%

des incidents détectés en 2022 concernent des entreprises de taille intermédiaire.

Source : Security Navigator 2023

Evaluer son niveau de sécurité

Aujourd'hui, aucune société n'est épargnée par la menace cyber. Selon le rapport Hiscox 2022, 48% des entreprises ont déjà été victimes d'une cyberattaque et une entreprise sur cinq a déclaré avoir risqué la faillite en conséquence. Les PME et ETI sont soumises aux mêmes menaces et se doivent de protéger leurs systèmes d'information.

Une offre adaptée aux PME/ETI

Les PME sont aujourd'hui en première ligne de la cybercriminalité. Elles sont le plus souvent impactées par :

- L'atteinte à la réputation
- La perte de clients
- L'interruption de la production
- Le vol de données clients
- La perte financière suite à escroquerie

Notre réponse : Cyber Diagnostic

Un diagnostic organisationnel des pratiques de sécurité

Permettant d'évaluer la maturité de l'organisation et d'identifier les écarts vis-à-vis des bonnes pratiques.

Un diagnostic technique

Sous la forme de tests techniques reproduisant les conditions d'une cyberattaque et permettant d'identifier toute vulnérabilité qui affecte le système d'information.

Un plan d'action

Vous permettant de mettre en place des mesures de sécurité adaptées à votre échelle, sur le court et le long terme.

Une déclinaison en 2 offres

Standard

- Diagnostic organisationnel
- Diagnostic technique interne du système d'information

Ou

- Diagnostic technique externe d'une adresse IP publique
- Plan d'action

Premium

- Diagnostic organisationnel
- Diagnostic technique interne du système d'information

Et

- Diagnostic technique externe d'une adresse IP publique
- Plan d'action

Options additionnelles

- Diagnostic technique Wi-Fi
- Diagnostic technique supplémentaire
- Campagne de phishing
- Veille en fuite de données
- Audit de configuration d'un ou plusieurs composants
- Contre-audit

Le processus

1. Cadrage de la prestation

- Recueillir les besoins
- Plannifier la mission

2. Diagnostic organisationnel et technique

- Recueillir la documentation
- Réaliser des entretiens ciblés
- Identifier et démontrer les vulnérabilités présentes

3. Consolidation des résultats

- Rédiger le rapport d'audit
- Elaborer un plan d'action

4. Restitution

- Présenter les résultats
- Elaborer la feuille de route

Vos bénéfices

- Etablir un état des lieux du niveau de sécurité du système d'information.
- Evaluer le niveau de conformité aux bonnes pratiques.
- Vérifier la robustesse de l'infrastructure vis-à-vis d'un attaquant.
- Fournir un plan d'action priorisé.

Pourquoi Orange Cyberdefense ?

- Des consultants certifiés avec plus de 10 ans d'expérience qui interviennent pour tout type d'organisations (PME, PMI, grands comptes, collectivités et administrations).
- Une démarche qui s'inscrit dans un cadre déontologique strict garantissant la probité des actions réalisées et la confidentialité de l'ensemble de vos données.
- Une action nourrie par notre connaissance de la menace.

Pour en savoir plus, contactez : **info@orangecyberdefense.com**
Nous suivre : **https://orangecyberdefense.com/fr**