# La checklist de l'offboarding sécurisé : les actions non négociables

**Offboarding sécurisé : ce que chaque départ dit de votre maturité cyber**


Whaller

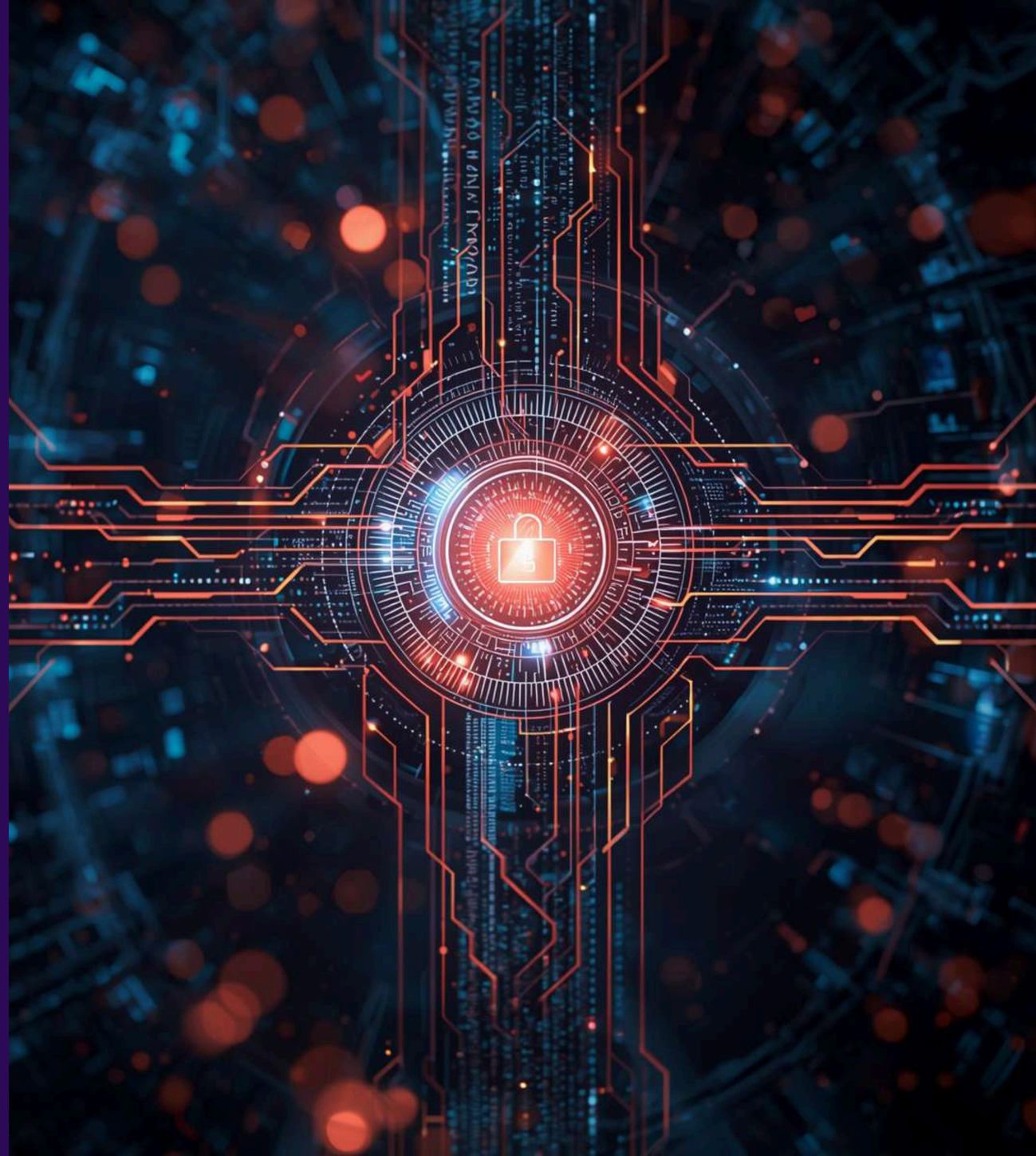
# Accès physiques

- Récupérer le badge d’accès aux locaux avant ou le jour du départ, sans exception
- Désactiver les codes d’alarme ou les accès biométriques associés au collaborateur
- Récupérer les clés physiques, cartes de stationnement, jetons d’accès
- Récupérer tout matériel professionnel : ordinateur portable, smartphone, tablette, supports de stockage amovibles

Whaller

# Accès au système d’information

- Désactiver le compte Active Directory ou LDAP immédiatement, sans attendre la fin du préavis si le collaborateur quitte physiquement les locaux
- Révoquer tous les accès VPN et connexions distantes
- Désactiver la messagerie professionnelle et mettre en place un renvoi temporaire si nécessaire pour la continuité d’activité, avec une durée définie et limitée
- Supprimer ou désactiver les comptes sur tous les outils SaaS métiers : CRM, ERP, outils de gestion de projet, plateformes collaboratives, outils marketing, etc.
- Révoquer les accès aux espaces de stockage partagé : serveurs de fichiers, drives, boxes documentaires
- Retirer les droits d’accès aux dépôts de code source si le collaborateur était développeur
- Révoquer les tokens d’API et les accès programmatiques éventuellement générés par le collaborateur



Whaller

# Mot de passe et secrets partagés

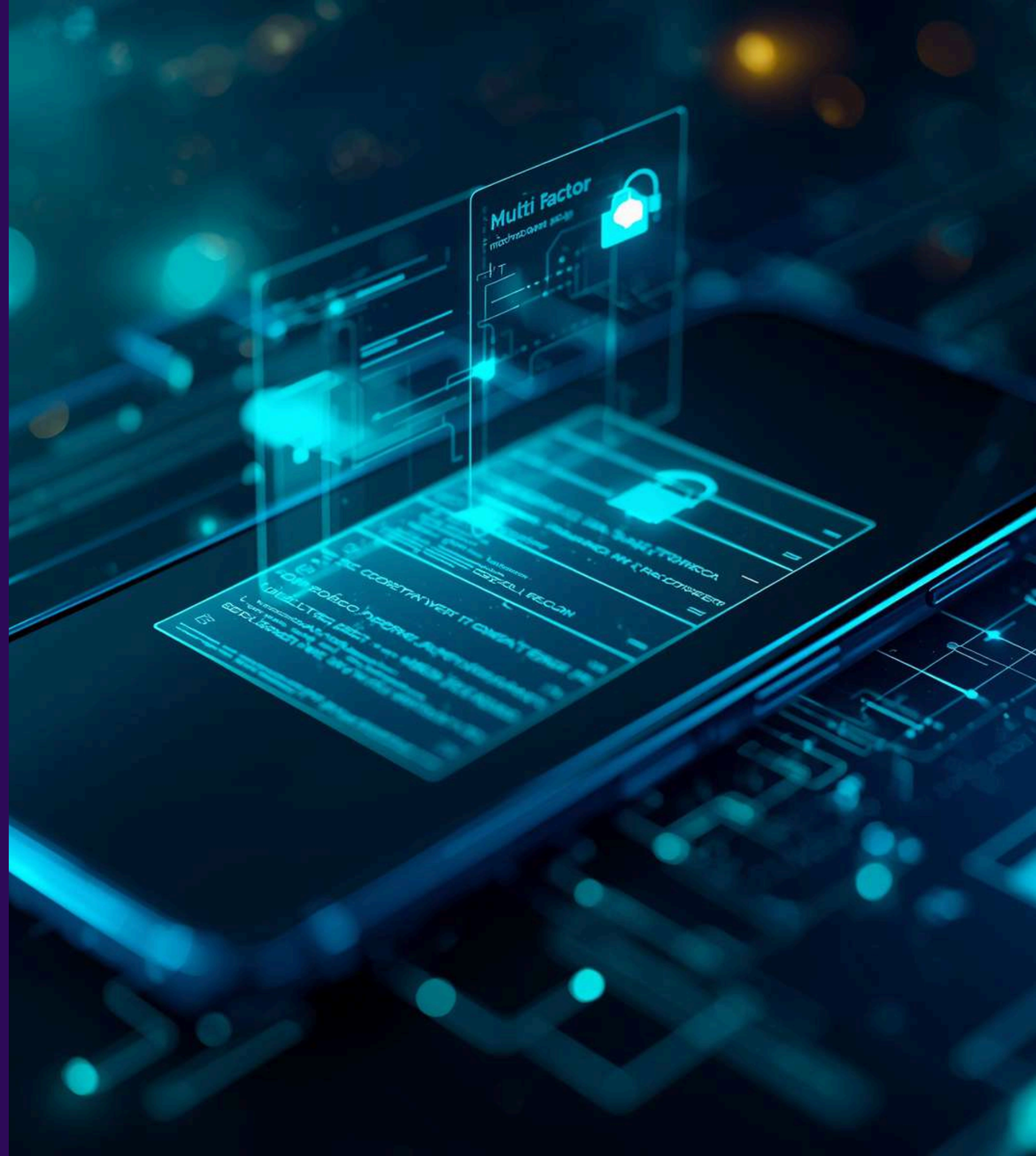
- Identifier toutes les applications auxquelles le collaborateur avait accès avec des identifiants partagés (boîtes mail génériques, comptes réseaux sociaux de l'entreprise, accès prestataires communs, etc.)
- Renouveler systématiquement tous ces mots de passe partagés
- Révoquer les accès aux gestionnaires de mots de passe d'équipe si le collaborateur y avait accès
- Changer les codes Wi-Fi si des codes d'accès réseau ont été communiqués

Whaller

# Authentification multi-facteurs (MFA)

- Désactiver les applications d’authentification liées aux comptes professionnels du collaborateur (Google Authenticator, Microsoft Authenticator, etc.)
- Révoquer les numéros de téléphone personnels enregistrés comme second facteur sur des applications professionnelles
- Régénérer les codes de secours MFA sur les comptes sensibles concernés

Whaller



# Comptes avec droits élevés : une vigilance particulière

- Révoquer les droits d’administration avant même le départ physique du collaborateur
- Transférer les droits et responsabilités à une autre personne habilitée
- Changer les mots de passe des comptes de service gérés par ce collaborateur
- Auditer les actions réalisées dans les jours précédant le départ sur les systèmes critiques

Whaller

# Après le départ : surveiller, auditer, documenter

- Surveiller les tentatives de connexion avec les anciens identifiants du collaborateur
- Paramétrer des alertes sur toute activité suspecte liée aux comptes récemment désactivés
- Vérifier que les transferts d’e-mails temporaires n’ont pas été détournés vers une adresse externe non autorisée
- Réaliser un audit complet dans les systèmes pour s’assurer qu’aucun accès résiduel n’a été oublié

Whaller

# Whaller

Email : contact@whaller.com Tél. : +33 1 47 92 82 18 Site web : whaller.com/fr