CYBERTELL / CHECKLIST POUR DÉMARRER AVEC CYBERTELL

Checklist pour démarrer avec CyberTell

Ce que votre entreprise prépare avant la configuration. Avec ces informations, la mise en place se fait en une seule séance.

Étape par étape · 8 étapes

01 **Désigner un interlocuteur et le premier administrateur**

Une personne qui gère CyberTell pour l'entreprise : prénom, nom et une adresse e-mail professionnelle personnelle. La connexion se fait par lien e-mail et passkey, sans mot de passe.

02 **Créer une boîte security@**

Créer une boîte ou une redirection **security@votre-domaine.ch** qui reçoit les e-mails de manière fiable et qui est consultée régulièrement. CyberTell y envoie la confirmation de votre domaine. L'adresse sert aussi de point de contact pour les incidents de sécurité.

> ! Sans boîte security@ fonctionnelle, le domaine ne peut pas être confirmé.

03 **Préparer le domaine et DMARC**

Définir le domaine principal de l'entreprise et clarifier l'accès à la gestion DNS. Pour l'analyse DMARC, créer un enregistrement TXT sur **_dmarc.votre-domaine.ch** avec CyberTell comme destinataire des rapports :

```
v=DMARC1; p=none; rua=mailto:dmarc@cybertell.io
```

04 **Envoi d'e-mails pour les simulations de phishing**

Les e-mails de phishing simulés passent par votre propre serveur de messagerie. À préparer : hôte SMTP, port (généralement 587), utilisateur, mot de passe, adresse et nom de l'expéditeur. SPF et DMARC doivent être configurés pour le domaine expéditeur ; DKIM est recommandé.

05 **Autoriser les simulations dans le filtre de messagerie**

Pour que les e-mails de test arrivent, autoriser votre serveur SMTP et le domaine expéditeur dans le filtre : dans Microsoft 365 via « Remise avancée » (simulation de phishing), dans Google Workspace via une liste d'autorisation. En option, un domaine de suivi propre : enregistrement TXT **_cybertell-verify.votre-domaine.ch** et un CNAME vers la cible affichée dans le portail. Autoriser aussi ce domaine.

06 Liste des collaborateurs en CSV

Tous les collaborateurs avec prénom, nom et adresse e-mail professionnelle, la langue en option (de, en, fr, it). Format : séparateur point-virgule, UTF-8, 2 Mo au maximum. Chaque adresse e-mail doit être unique.

```
firstname;lastname;email;language
Max;Muster;max.muster@example.ch;de
```

07 Profil de l'entreprise et environnement IT

Logo, site web et une brève description de l'entreprise. Pour la première évaluation des risques, noter : systèmes utilisés (Windows, Active Directory, Microsoft 365, macOS, Linux), pare-feu et protection des terminaux, fournisseurs importants et lieux de traitement des données personnelles.

08 Optionnel : intégrations

Pour le raccordement au SOC : accès au pare-feu (Sophos, Firewalla, pfSense) ou un enregistrement d'application dans Microsoft Entra ID pour Defender. En plus, un webhook Slack pour les alertes et un plan de déploiement de l'app CyberTell sur les appareils des collaborateurs.

Prêt à démarrer lorsque ...

- [ ] le premier administrateur est désigné et son adresse e-mail fonctionne
- [ ] security@votre-domaine.ch reçoit des e-mails
- [ ] l'accès à la gestion DNS est clarifié
- [ ] les accès SMTP pour les simulations sont disponibles
- [ ] la liste des collaborateurs est prête en CSV