

## PHASE 1A : DIAGNOSTIC



### ETAT DES LIEUX

Questionnaire d'auto-évaluation pour effectuer un **état des lieux complet** de votre cybersécurité.  
**Rapport** détaillé avec feuille de route.



### SEANCE DE DIAGNOSTIC

Séance avec un-e **auditeur-ice** pour passer en revue votre état des lieux, vous **conseiller** et vous **orienter** sur la suite du processus.



### SCANS DE VULNERABILITES

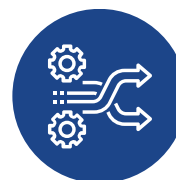
Scans internes et externes pour **identifier et signaler des failles** dans vos infrastructures informatiques.  
**Rapport** de vulnérabilités détaillé.



### CAMPAGNE DE PHISHING

Envois d'**e-mails** frauduleux pour **sensibiliser** vos équipes et partage de ressources de formations.  
**Rapport** de phishing détaillé.

## PHASE 1B : PLAN D' ACTIONS



### RAPPORT CYBERRISQUES

Rapport détaillé de vos **cyberrisques**, des **mesures de remédiations** et **recommandations d'améliorations**.



### SEANCE DE REMEDIATION

Séance avec un-e **auditeur-ice** pour passer en revue **vos priorités**, les mesures correctives demandées et **préparer l'audit cybersécurité**.

## PHASE 2 : AUDIT & LABELLISATION



### AUDIT CYBERSECURITE

Un-e auditeur-ice **vérifie** l'implémentation des **mesures de cybersécurité** de votre organisation.  
**Rapport** d'audit final complet.



### LABEL CYBER-SAFE

Obtention du **Label Cyber-Safe** pour deux ans en cas d'audit réussi et d'**avantages** avec les partenaires du Label.

