FICHE DE RÉVISION

Module : Sensibilisation et Formation des Équipes

Formation : Pilotage et Animation de la Cybersécurité

🧠 1. Introduction à la Culture Cybersécurité

> **Objectif :** Comprendre les enjeux humains et les leviers d'adhésion

▸ Le facteur humain au coeur des risques cyber

> 80 %

des incidents de sécurité impliquent un facteur humain

(erreur, négligence ou manipulation)

Types d'erreurs humaines en cybersécurité :

- Erreur non intentionnelle : mauvais destinataire, clic accidentel
- Négligence : mot de passe faible, mise à jour ignorée
- Manipulation : phishing, pretexting, vishing
- Malveillance interne : initié mécontent ou motivé

▸ Qu'est-ce que la culture cybersécurité ?

La culture cybersécurité désigne l'ensemble des valeurs, comportements, connaissances et réflexes partagés par les membres d'une organisation face aux risques numériques. Elle transforme la sécurité d'une contrainte imposée en un réflexe collectif et partagé.

Niveau de culture	Caractéristiques observables
🔴 Inexistante / Réactive	Les incidents sont traités au cas par cas ; aucune règle formalisée ; sécurité perçue comme une contrainte IT
🟠 Émergente	Des règles existent (charte, PSSI) mais sont peu connues ; sensibilisation sporadique ; engagement limité de la direction
🟡 En développement	Programme de sensibilisation en place, formations régulières, quelques référents sécurité dans les métiers
🟢 Mature	Sécurité intégrée dans tous les processus, signalement spontané d'incidents, direction exemplaire, culture partagée
🔵 Optimisée	Amélioration continue, benchmark, partage de bonnes pratiques en interne et avec le secteur, ambassadeurs sécurité actifs

▸ Les leviers d'adhésion — Facteurs clés de succès

Levier	Principe	Mise en oeuvre concrète
Exemplarité de la direction	La direction doit être la première à respecter et à afficher les bonnes pratiques cyber	Le DG participe aux formations, valide la PSSI publiquement, évoque la cybersécurité en réunion d'équipe
Pertinence des messages	Les exemples utilisés parlent au quotidien des collaborateurs, pas aux techniciens	Illustrer avec des incidents réels du secteur, des cas concrets du métier de l'interlocuteur
Répétition et régularité	La sécurité s'installe dans les habitudes par la répétition espacée — pas par une formation unique	Programme annuel d'actions récurrentes : campagnes phishing, newsletters, quiz mensuels

Récompense et gamification	Valoriser les bons comportements plutôt que sanctionner les erreurs — le cerveau retient mieux la récompense	Classements, badges, récompenses pour les meilleurs scores aux quiz ou taux de signalement
Réseau d'ambassadeurs	Des relais de confiance dans les équipes diffusent les messages avec crédibilité et proximité	Former des référents sécurité volontaires dans chaque direction, département ou site
Droit à l'erreur assumé	Sanctionner la négligence sans pédagogie crée la peur et le silence — les erreurs doivent être signalées sans crainte	Communication claire : signaler une erreur ou un clic sur un lien suspect ne mène pas à une sanction

▸ Obligations réglementaires de sensibilisation

Réglementation	Article / Mesure	Exigence en matière de sensibilisation
RGPD	Art. 32 + 39	Mesures de sensibilisation du personnel traitant des données personnelles ; rôle du DPO dans la sensibilisation
NIS2	Art. 21 §2 (g)	Formation obligatoire des membres des organes de direction et du personnel aux cyber-risques
ISO 27001:2022	Annexe A — A.6.3	Sensibilisation, éducation et formation à la sécurité de l'information pour tout le personnel
LPM / Qualification ANSSI	Guides ANSSI	Les OIV/OSE doivent sensibiliser leurs équipes aux bonnes pratiques de l'hygiène informatique
DORA (secteur financier)	Art. 5	Programme de sensibilisation aux risques TIC et aux cybermenaces pour l'ensemble du personnel

🔎 2. Diagnostic du Niveau de Maturité Cyber

> **Objectif :** Identifier les besoins de formation et les populations cibles

▸ Les sources du diagnostic de maturité sensibilisation

Source de données	Méthode de collecte	Informations obtenues
Analyse des incidents passés	Revue des tickets d'incidents sur 12 mois	Part des incidents liés au facteur humain, types d'erreurs récurrentes, populations impliquées
Campagne de phishing simulé (baseline)	Envoi d'un email de test sans formation préalable	Taux de clic initial par direction, taux de signalement, profil des utilisateurs les plus vulnérables
Questionnaire de maturité	Sondage en ligne sur les connaissances et pratiques	Niveau de connaissance des règles (PSSI, mots de passe, BYOD), perception du risque cyber
Entretiens avec les managers	Interviews semi-directifs par direction ou métier	Risques spécifiques au métier, comportements observés, freins à la sécurité, besoins exprimés
Audit de conformité PSSI	Revue documentaire et observations terrain	Écarts entre les règles formalisées et les comportements réels — base pour la priorisation

Résultats des formations existantes	Analyse des taux de complétion et des scores	Sujets maîtrisés vs. lacunes identifiées, populations n'ayant pas suivi les formations

▸ Segmentation des populations cibles

Population cible	Profil de risque	Besoins spécifiques	Priorité de formation
Direction Générale / COMEX	Cibles de spear phishing, décideurs engagement budgétaire cyber	Enjeux stratégiques et réglementaires (NIS2, DORA), responsabilité personnelle, ROI de la sécurité	🔴 Haute — formation courte, présentielle, personnalisée
Équipes IT et administrateurs SI	Comptes privilégiés, vecteurs d'attaque internes, supply chain	Sécurité by design, gestion des accès privilégiés, réponse à incident, habilitations	🔴 Haute — formation technique avancée, certifications
Services Finance / Comptabilité	Cibles de fraudes au virement (CEO Fraud, BEC), manipulation données financières	Vérification des ordres de virement, validation des RIB, signalement d'anomalies	🔴 Haute — focus arnaque au président, procédures anti-fraude
RH / DPO / Juridique	Traitent des données sensibles (contrats, paye, données personnelles)	RGPD appliqué à leur métier, gestion des droits des personnes, données sensibles	🟠 Élevée — focus RGPD, confidentialité, gestion des accès
Commerciaux / Relation client	Mobilité, utilisation d'appareils perso, contacts clients à protéger	Hygiène numérique en déplacement, protection des données clients, phishing	🟠 Élevée — focus mobilité, phishing, protection des données
Tous collaborateurs (socle commun)	Vecteur d'entrée phishing, erreurs courantes, BYOD, télétravail	Bonnes pratiques de base : mots de passe, mise à jour, signalement, données personnelles	🟡 Standard — e-learning obligatoire, campagnes régulières
Prestataires et sous-traitants	Accès au SI avec risque de rebond, soumis aux clauses contractuelles	Obligations contractuelles, gestion des accès, conduite à tenir en cas d'incident	🟡 Standard — sensibilisation spécifique aux règles d'accès
Nouveaux arrivants (onboarding)	Méconnaissance totale des règles internes et des risques spécifiques	Découverte de la PSSI, charte informatique, procédures de signalement, contacts utiles	🔴 Immédiate — avant tout accès au SI

▸ Grille de scoring — Priorisation des besoins de formation

Population / Direction	Exposition au risque (1-4)	Niveau de maturité (1-4 inversé)	Impact métier (1-4)	Score total (/12)	Action prioritaire
Finance / Comptabilité	4	3 (faible maturité)	4	11	Formation anti-fraude immédiate + procédures

Administrateurs SI	4	2	4	10	Formation technique avancée + certifications
Direction Générale	4	3	3	10	Sensibilisation dirigeants + exercice de crise
Commerciaux / Terrain	3	3	3	9	E-learning phishing + kit mobilité
Tous collaborateurs	2	2	2	6	E-learning socle commun annuel obligatoire

3. Conception d'un Plan de Formation Interne

> **Objectif :** Définir les objectifs, contenus, supports et modalités

Structure type d'un plan de formation cybersécurité annuel

#	Étape	Contenu et livrables
1	Diagnostic initial	Analyse des incidents, campagne phishing baseline, questionnaire de maturité — Livrable : rapport de diagnostic
2	Définition des objectifs	Par population : objectifs SMART (Spécifique, Mesurable, Atteignable, Réaliste, Temporel) — Livrable : matrice objectifs / populations
3	Conception du programme	Thèmes, contenus, modalités pédagogiques, durées, supports — Livrable : programme détaillé par population
4	Sélection des prestataires / outils	Évaluation des solutions LMS, prestataires de phishing simulé, prestataires animation — Livrable : cahier des charges
5	Calendrier et planification	Répartition des actions sur 12 mois, jalons, ressources mobilisées, budget — Livrable : calendrier annuel validé
6	Communication du lancement	Message de la direction, présentation du programme aux managers, page intranet dédiée — Livrable : kit de communication
7	Déploiement	Lancement des modules e-learning, ateliers, campagnes, événements — Livrable : indicateurs de participation en temps réel
8	Mesure et bilan	Analyse des indicateurs d'impact, bilan quantitatif et qualitatif, présentation à la direction — Livrable : rapport bilan annuel

Les thèmes de formation par niveau de priorité

Priorité	Thème de formation	Population prioritaire	Format recommandé
🔴 Fondamental	Phishing, hameçonnage et ingénierie sociale	Tous collaborateurs	E-learning + phishing simulé trimestriel
🔴 Fondamental	Mots de passe et authentification forte (MFA)	Tous collaborateurs	Module e-learning court + vidéo tuto MFA
🔴 Fondamental	Signalement d'incident et conduite à tenir	Tous collaborateurs	Fiche réflexe + quiz + onboarding obligatoire

🟠 Prioritaire	Télétravail et mobilité sécurisée	Tous collaborateurs	E-learning + kit bonnes pratiques imprimable
🟠 Prioritaire	Fraude au virement et arnaque au président (CEO Fraud)	Finance, Direction, Assistantes	Atelier présentiel + mise en situation
🟠 Prioritaire	Protection des données personnelles (RGPD)	RH, Marketing, Relation client	E-learning RGPD + guide pratique métier
🟡 Important	Classification et gestion des données sensibles	Tous + focus sur métiers traitant de données critiques	Module e-learning + cheat sheet
🟡 Important	Sécurité des applications et du cloud (usage pro)	Équipes techniques et managers	Webinaire + guide cloud sécurisé
🔵 Avancé	Enjeux cyber pour les dirigeants et responsabilité légale	COMEX, Direction Générale	Séminaire exécutif demi-journée, cas réels
🔵 Avancé	Sécurité by design, développement sécurisé (OWASP)	Équipes IT / Développement	Formation technique certifiante (3 jours)

▸ Rédiger des objectifs pédagogiques SMART

Lettre	Critère	Exemple appliqué à la cybersécurité
S — Spécifique	L'objectif décrit un comportement observable et précis	À l'issue de la formation, le collaborateur est capable d'identifier un email de phishing et de le signaler via le bouton dédié
M — Mesurable	Un indicateur permet de vérifier l'atteinte de l'objectif	Taux de clic sur campagne de phishing simulé < 5 % à 3 mois après la formation
A — Atteignable	L'objectif est réaliste au regard du public et des ressources	Une formation de 20 min accessible sur mobile pour des commerciaux terrain non techniques
R — Réaliste / Pertinent	L'objectif répond à un besoin réel identifié dans le diagnostic	Focus anti-phishing pour la Direction Finance suite à 3 tentatives de fraude au virement détectées
T — Temporellement défini	Un délai clair est fixé pour l'atteinte de l'objectif	100 % du personnel formé avant le 30 juin ; réévaluation par campagne phishing en septembre

🛠️ 4. Outils et Méthodes de Sensibilisation

> **Objectif :** Découvrir les supports numériques, campagnes et jeux sérieux

▸ Panorama des formats de sensibilisation — Comparatif

Format	Durée type	Avantages	Limites	Meilleur usage
E-learning / LMS	15-30 min / module	Scalable, traçable, disponible 24/7, coût faible à l'unité	Engagement limité, risque de zapping, efficacité variable selon la qualité	Socle commun obligatoire, onboarding, RGPD, hygiène numérique

Phishing simulé	Campagne 2-4 semaines	Mesure réelle du comportement, pédagogie au moment de l'erreur, forte mémorisation	À cadrer éthiquement, peut être vécu comme un piège si mal communiqué	Mesure de la maturité, entraînement régulier (min. 2 fois/an)
Atelier présentiel	2-4 heures	Interactif, adapté au contexte métier, questions/réponses, réseau d'échanges	Chronophage, coûteux à grande échelle, nécessite un animateur expert	Populations à risque élevé, Finance, Dirigeants, IT, nouvelles recrues
Serious game / Escape game cyber	1-3 heures	Très engageant, mémorisation élevée, esprit d'équipe, dédramatise la cyber	Coût de conception élevé, animation nécessaire, non scalable facilement	Événements fédérateurs, journée sécurité, groupes de 5-12 personnes
Vidéo courte (micro-learning)	2-5 min	Format adapté au mobile, attention maximale, facilement mémorisable, partage facile	Production coûteuse si sur-mesure, obsolescence rapide, pas de mesure d'impact direct	Rappels mensuels, actualité cyber, bonnes pratiques visuelles
Newsletter / intranet sécurité	Hebdo ou mensuel	Large diffusion, faible coût, maintient la sécurité dans le radar des équipes	Taux d'ouverture variable, impact comportemental difficile à mesurer	Veille, actualité incidents, rappels de bonnes pratiques, alertes
Quiz / Évaluations en ligne	5-15 min	Mesure des connaissances, gamification facile, identification des lacunes	Ne garantit pas le changement de comportement réel	Tests pré/post formation, certification interne, concours sécurité
Affichage / Poster	Permanent	Visibilité continue, faible coût, rappel visuel au bureau et en salle de pause	Impact comportemental très limité seul, ne suffit pas comme unique action	Complément visuel, campagne thématique, affichage des 10 règles clés

▸ La campagne de phishing simulé — Mode d'emploi

#	Étape	Détail et bonnes pratiques
1	Cadrage éthique et juridique	Information des instances représentatives (CSE) et de la direction ; communication préalable sur le principe (pas sur le calendrier) ; définir la finalité pédagogique — jamais sanctionnelle
2	Définition du scénario	Choisir un scenario réaliste pour l'organisation (facture, demande RH, livraison colis, alerte sécurité) — calibrer la difficulté selon le niveau initial
3	Paramétrage de la campagne	Configurer la plateforme (GoPhish, KnowBe4, Proofpoint, Sophos Phish Threat), créer la landing page pédagogique déclenchée au clic
4	Mesure des résultats	Collecter : taux d'ouverture, taux de clic sur le lien, taux de saisie de credentials, taux de signalement — par direction et par profil
5	Page de sensibilisation immédiate	Afficher immédiatement au clic un message pédagogique clair : 'Vous venez de cliquer sur un lien de test — voici comment l'éviter la prochaine fois'

6	Analyse et bilan	Restitution des résultats agrégés aux managers ; identification des populations à risque ; ajustement du plan de formation
7	Itération	Recommencer avec un scénario différent et de difficulté croissante — objectif : taux de clic < 5 % à 12 mois

▸ Le serious game cyber — Formats et cas d'usage

Type de serious game	Principe pédagogique	Cas d'usage idéal
Escape game cyber (présentiel)	Résoudre des énigmes liées à des incidents cyber en équipe en temps limité — apprend en faisant	Journée sécurité, team building, sensibilisation des dirigeants, groupes de 5 à 12
Simulation d'incident (table-top)	Scénario de crise joué en rôles : RSSI, DG, Communication, métiers — teste les réflexes et procédures	Exercice annuel de crise cyber, test du PCA, formation de la cellule de crise
Jeu de cartes (Crypt..), wargame	Questions/réponses gamifiées sur les thèmes de la cybersécurité — compétition individuelle ou par équipe	Animation d'équipe, réunion mensuelle, quiz inter-services, onboarding ludique
Serious game en ligne (app / LMS)	Parcours narratif interactif où les choix du joueur ont des conséquences sur un scénario cyber fictif	Formation à distance, onboarding digital, sensibilisation des populations dispersées

5. Animation et Communication Interne

> **Objectif :** Développer des messages adaptés aux différents publics

▸ Adapter le message à la cible — Règle d'or de la communication sécurité

Le même message technique délivré à tous les publics est inefficace. Le RSSI doit adopter la posture du communicant : comprendre les préoccupations, le vocabulaire et les enjeux de chaque interlocuteur pour construire un message qui résonne avec sa réalité.

Cible	Ce qui les motive / les préoccupe	Message cybersécurité adapté
Direction Générale	Performance, réputation, responsabilité légale, coûts	« Un incident cyber coûte en moyenne X M€ et 3 semaines d'arrêt — la conformité NIS2 protège aussi la réputation de l'entreprise »
Managers / Encadrement	Efficacité de l'équipe, atteinte des objectifs, gestion du risque opérationnel	« La cybersécurité, c'est aussi votre responsabilité : un collaborateur non formé peut bloquer l'équipe entière »
Finance / Comptabilité	Fiabilité des données, prévention des fraudes, contrôle interne	« Vérifiez toujours un RIB par téléphone avant tout virement — 40 % des fraudes au président visent votre métier »
Équipes IT	Performance technique, résolution de problèmes, enjeux professionnels	« La sécurité by design évite les correctifs urgents en production — intégrez l'OWASP Top 10 dès la conception »

Tous collaborateurs	Simplicité, vie quotidienne numérique, vie privée, peur de faire des erreurs	« Signaler un email suspect, c'est protéger l'entreprise — vous ne serez pas puni pour avoir prévenu »
Prestataires / Tiers	Maintien du contrat, respect des obligations, risque de responsabilité	« Vos accès sont tracés et vos obligations de sécurité sont contractuelles — voici les règles à respecter »

▸ Plan d'animation annuel — Les 12 mois de la cybersécurité

Période	Action principale	Format	Cible
Janvier	Lancement du programme annuel + formation onboarding vague 1	Email DG + e-learning LMS	Tous + nouveaux arrivants
Février	Campagne phishing simulé #1 (baseline ou difficile progressive)	Phishing simulé + landing page péda.	Tous collaborateurs
Mars	Formation spécifique Finance/Compta — Fraude au virement	Atelier présentiel 2h + procédure anti-fraude	Finance, DG, Assistantes
Avril	Module e-learning RGPD obligatoire	E-learning 30 min — relances auto LMS	RH, Marketing, Juridique
Mai	Cybermois interne — Semaine de la cybersécurité	Quizz, affichage, vidéos, démo phishing live	Tous collaborateurs
Juin	Formation IT — Sécurité by design et gestion des accès privilégiés	Formation technique 1 journée	DSI, Administrateurs
Juillet-Août	Newsletter sécurité spéciale vacances (Wi-Fi public, voyages, BYOD)	Email + affiche départ vacances	Tous collaborateurs
Septembre	Campagne phishing simulé #2 + mesure de progression	Phishing simulé + rapport d'évolution	Tous collaborateurs
Octobre	Mois européen de la cybersécurité (ECSM) — Événement fédérateur	Escape game cyber, conférence invité, quiz inter-équipes	Tous + Direction
Novembre	Sensibilisation dirigeants — Exercice de crise table-top	Séminaire exécutif demi-journée	COMEX, DG, RSSI
Décembre	Bilan annuel + restitution des indicateurs à la direction	Rapport annuel + présentation COMEX	Direction, RSSI, DSI
Continu	Newsletter mensuelle, actualité cyber, alertes CERT-FR pertinentes	Email / Intranet	Tous collaborateurs

Le réseau d'ambassadeurs cyber — Organisation et animation

- Recruter des volontaires dans chaque direction / département / site — profils communicants, curieux, respectés
- Former les ambassadeurs en priorité : formation avancée (1 journée) + accès aux outils et aux actualités RSSI
- Rôle des ambassadeurs : relayer les messages, recueillir les questions terrain, signaler les comportements à risque, animer les quiz locaux
- Valoriser leur engagement : reconnaissance interne, invitation aux séminaires, badge 'Ambassadeur Cyber', mention dans le rapport annuel
- Fréquence des réunions ambassadeurs : trimestriel minimum — partage des actualités, retours terrain, préparation des prochaines actions

6. Évaluation et Amélioration Continue

> **Objectif :** Définir les indicateurs d'impact et formaliser le retour d'expérience

Pourquoi mesurer l'impact de la sensibilisation ?

Sans mesure, il est impossible de démontrer la valeur du programme, d'identifier les populations encore fragiles ou d'obtenir les budgets nécessaires. La mesure de la sensibilisation suit la même logique que les indicateurs de sécurité : ce qui ne se mesure pas ne s'améliore pas.

Tableau de bord des indicateurs de sensibilisation

Indicateur	Description	Cible	Fréquence	Source
Taux de clic phishing simulé	% d'utilisateurs ayant cliqué sur un lien de phishing simulé	< 5 % à 12 mois	Trimestriel	Plateforme phishing
Taux de signalement phishing	% d'utilisateurs ayant signalé le mail via le bouton dédié	> 30 %	Trimestriel	Plateforme phishing
Taux de complétion e-learning	% de collaborateurs ayant finalisé les modules obligatoires	> 90 %	Mensuel	LMS
Score moyen aux quiz	Note moyenne obtenue aux évaluations de connaissance	> 75 % / quiz	Par campagne	LMS / Quiz tool
Taux de signature de la charte	% de collaborateurs ayant signé la charte informatique	100 %	Annuel	RH / RSSI
Nb d'incidents liés au facteur humain	Nombre d'incidents causés par une erreur ou négligence humaine	Tendance ↓ vs N-1	Mensuel	Ticketing sécurité
Nb de signalements spontanés d'incidents	Nombre d'incidents signalés par des utilisateurs non IT	Tendance ↑	Mensuel	Ticketing sécurité
Taux de satisfaction formation	Note de satisfaction des participants après formation	> 4/5	Par action	Questionnaire post-formation
Taux de participation aux événements	% de collaborateurs ayant participé aux événements cyber (Cybermois, escape game…)	> 60 %	Annuel	Registre participants
Couverture du plan de formation	% d'actions du plan réalisées dans les délais prévus	> 85 %	Trimestriel	Plan de formation

▸ Le modèle de Kirkpatrick — Évaluation à 4 niveaux

Le modèle de Kirkpatrick (adapté à la formation) permet d'évaluer l'impact réel d'une action de sensibilisation au-delà de la simple satisfaction.

Niveau	Dimension	Question clé	Méthode de mesure en cybersécurité
1	Réaction	Les apprenants ont-ils apprécié la formation ?	Questionnaire de satisfaction à chaud (immédiatement après la formation) — note et commentaires
2	Apprentissage	Les apprenants ont-ils acquis les connaissances et compétences visées ?	Quiz de connaissance avant/après (pré-test / post-test) — mesure de la progression du score
3	Comportement	Les apprenants appliquent-ils dans leur travail ce qu'ils ont appris ?	Campagne de phishing simulé post-formation, observation du taux de signalement, revue des incidents
4	Résultats	La formation a-t-elle eu un impact mesurable sur la sécurité de l'organisation ?	Évolution du nombre d'incidents liés au facteur humain, ROI de la sensibilisation vs coût d'un incident

▸ Formaliser le rapport bilan annuel de sensibilisation

§	Rubrique	Contenu
1	Synthèse exécutive	Résumé en 1 page : taux de clic phishing N vs N-1, couverture du plan, faits marquants, bilan en 3 indicateurs clés
2	Réalisation du plan d'actions	Tableau de bord des actions prévues vs réalisées, taux de complétion, raisons des écarts
3	Résultats des campagnes phishing	Évolution du taux de clic et de signalement par campagne et par direction (graphique de tendance)
4	Résultats des formations e-learning	Taux de complétion par module et par population, scores moyens, populations en retard identifiées
5	Impact sur les incidents	Évolution du nombre d'incidents liés au facteur humain — corrélation avec les actions de sensibilisation menées
6	Axes d'amélioration	Populations encore fragiles, thèmes à renforcer, nouveaux formats à tester, budget demandé pour N+1
7	Plan d'action N+1	Programme prévisionnel, objectifs SMART, budget prévisionnel, calendrier, validation demandée à la direction

▸ RETEX et amélioration continue du programme de sensibilisation

- Analyser les incidents liés au facteur humain pour ajuster les thèmes de formation (nouvelle menace = nouveau module)
- Recueillir les retours des managers et des ambassadeurs sur la pertinence des messages et des formats
- Comparer les indicateurs avec les benchmarks sectoriels (ex. : rapports Verizon DBIR, Proofpoint State of the Phish)
- Adapter le niveau de difficulté des campagnes phishing à la progression observée — ne pas rester sur des scénarios trop faciles
- Réviser le plan de formation a minima annuellement et après chaque incident significatif impliquant un facteur humain
- Présenter le bilan à la direction et au COPIL sécurité pour obtenir la validation du plan N+1 et des ressources associées

📌 Mémo Récapitulatif — À Retenir

🧠 Culture Cyber	🔎 Diagnostic	📐 Plan de Formation	🛠️ Outils & Méthodes	📣 Animation	📈 Évaluation
• > 80 % des incidents = facteur humain • 5 niveaux de culture (Inexistante → Optimisée) • 6 leviers d'adhésion (exemplarité DG, droit à l'erreur…) • NIS2 : formation dirigeants obligatoire • ISO 27001 A.6.3 : formation tracée obligatoire	• 6 sources de diagnostic • 8 populations cibles (DG, IT, Finance, tous…) • Finance = priorité : cibles CEO Fraud • Onboarding = formation immédiate avant accès SI • Scoring : exposition + maturité inversée + impact	• 8 étapes du plan (diagnostic → bilan) • Objectifs SMART obligatoires • 10 thèmes classés par priorité • Phishing + MFA + signalement = socle fondamental • Formation dirigeants : courte, présentielle, personnalisée	• 8 formats comparés (e-learning, phishing, escape…) • Phishing simulé : 7 étapes + cadrage éthique (CSE) • Cible phishing : < 5 % de clic à 12 mois • Escape game : groupes 5-12, fort impact mémorisation • Micro-learning : 2-5 min, idéal mobile et rappels	• Adapter le message à chaque cible • Plan 12 mois : ECSM en octobre, phishing x2/an • Newsletter mensuelle = maintien dans le radar • Ambassadeurs : recrutement + formation + valorisation • Cybermois interne = événement fédérateur annuel	• Modèle Kirkpatrick : 4 niveaux (Réaction → Résultats) • 10 KPIs (clic, signalement, complétion, incidents…) • Rapport bilan annuel : 7 rubriques + validation DG • Taux signalement cible > 30 % • RETEX : adapter à chaque incident facteur humain

Le cycle vertueux de la sensibilisation

Diagnostic → Plan de formation → Déploiement des actions → Mesure de l'impact → RETEX → Amélioration du programme → Nouvelle campagne