

LIVRE BLANC

Culture cyber en entreprise : le guide

Faire de vos équipes votre première ligne de défense : sensibilisation, réflexes, gouvernance humaine et mesure, du plan au changement durable.

Sedona Radar — audit de sécurité externe automatisé

Sedona AI Lecture ~25 min Édition 2026 sedona-ai.com

Sommaire

01	1. Résumé exécutif : la culture cyber, dernier pare-feu et premier levier
02	2. L'humain au centre : ce que disent les données
03	3. Panorama chiffré de la menace 2024-2026 (France + Europe)
04	4. Vulgarisation : culture cyber vs sensibilisation ponctuelle
05	5. Ingénierie sociale et phishing décryptés
06	6. Cadre réglementaire et obligations
07	7. Le sponsor top-management : sans direction, pas de culture
08	8. Levier 1 — Formation continue et micro-learning
09	9. Levier 2 — Simulations de phishing : bonnes pratiques et pièges
10	10. Levier 3 — Onboarding et parcours par rôle
11	11. Levier 4 — Hygiène des accès : mots de passe, MFA, gestion des droits
12	12. Levier 5 — Télétravail, BYOD et mobilité
13	13. Méthode — Étape 1 : état des lieux initial et baseline
14	14. Méthode — Étape 2 : construire le plan de sensibilisation sur 12 mois
15	15. Méthode — Étape 3 : campagnes, KPIs et mesure
16	16. Méthode — Étape 4 : culture du signalement sans blâme (no-blame)
17	17. Ancrage durable : nudges, gamification, ambassadeurs
18	18. Les erreurs fréquentes qui sabotent la démarche
19	19. Spécificités PME/ETI : faire beaucoup avec peu
20	20. Checklist opérationnelle 30 / 60 / 90 jours
21	21. Modèles prêts à l'emploi
22	22. Où s'adresser, anticiper et retours d'expérience

La majorité des violations de données commence par un humain — un clic, une erreur de manipulation, un identifiant volé — et l'IA générative industrialise désormais l'ingénierie sociale. Face à cela, la plupart des organisations s'en tiennent à une formation annuelle unique dont l'effet durable est faible. Ce livre blanc distingue clairement la sensibilisation ponctuelle de la culture cyber, s'appuie en priorité sur des sources primaires 2024-2026 (Verizon, ENISA, IBM, ANSSI, CNIL, Cybermalveillance, CESIN, SANS), et déroule une méthode pas-à-pas — état des lieux, plan sur 12 mois, KPIs, culture du signalement sans blâme — assumant même ce que la recherche récente nuance sur les simulations de phishing.

À retenir

- Environ 60 % des violations impliquent un facteur humain : l'humain est à la fois la surface d'attaque n°1 et la meilleure ligne de défense (Verizon DBIR 2025).
- La sensibilisation ponctuelle (formation annuelle « case à cocher ») ne crée pas de culture : seule une cadence continue, mesurée et portée par la direction ancre des réflexes durables.
- Le phishing reste le premier vecteur d'accès initial, et plus de 80 % des e-mails de phishing récents intègrent de l'IA — les attaques deviennent plus rapides, plus crédibles, moins coûteuses à produire.
- NIS2 (article 20) prévoit de rendre la formation non optionnelle : responsabilité personnelle des dirigeants, formation des organes de direction et encouragement à former tous les salariés (directive non transposée en droit français au 14/10/2026).
- Mesurez le taux ET la rapidité de signalement, pas seulement le taux de clic : la recherche indépendante montre que des simulations mal conçues ou punitives donnent des gains marginaux, voire nuls.
- La culture du signalement sans blâme (no-blame) réduit le temps de détection : culpabiliser détruit la remontée d'alerte.
- Pour une PME/ETI sans RSSI, quatre quick wins à fort impact d'abord : MFA résistant au phishing, gestionnaire de mots de passe, signalement en 1 clic, kit gratuit Cybermalveillance.

01 1. Résumé exécutif : la culture cyber, dernier pare-feu et premier levier

La technologie seule ne protège plus. Pare-feux, EDR et filtres anti-spam sont nécessaires mais insuffisants dès lors que l'attaquant vise directement la personne : un e-mail bien tourné, un faux appel du dirigeant, un QR code piégé. L'humain est simultanément la première surface d'attaque et, correctement outillé, la meilleure ligne de défense. Ce livre blanc a un objectif unique : vous faire passer d'une sensibilisation ponctuelle à une culture cyber ancrée, mesurable et durable.

~60 %

des violations de données impliquent un facteur humain (erreur, manipulation ou usage malveillant).

Verizon, 2025 Data Breach Investigations Report

21 secondes

temps médian entre l'ouverture d'un e-mail de phishing et le premier clic sur un lien piégé.

Verizon, 2025 Data Breach Investigations Report

16 % / 4,8 M\$

le phishing est le premier vecteur d'accès initial (16 % des violations) ; une violation d'origine phishing coûte en moyenne 4,8 M\$.

IBM, Cost of a Data Breach Report 2025

À qui s'adresse ce livre blanc

Aux dirigeants (sponsors indispensables de la démarche, et visés par la responsabilité que NIS2 prévoit pour les dirigeants), aux DRH (onboarding, charte, parcours par rôle, culture interne), et aux DSI/RSSI (état des lieux, campagnes, KPIs, hygiène des accès). Il est pensé pour les PME et ETI qui doivent faire beaucoup avec peu, mais s'applique à toute organisation.

02 2. L'humain au centre : ce que disent les données

« Facteur humain » ne signifie pas « employé négligent ». Il recouvre trois réalités très différentes qu'il faut traiter distinctement, car les réponses ne sont pas les mêmes.

Catégorie	Description	Réponse dominante
Erreur non intentionnelle	Mauvais destinataire, pièce jointe sensible, mauvaise configuration, perte d'appareil.	Processus, garde-fous techniques, culture du signalement sans blâme.
Manipulation (ingénierie sociale)	La personne est trompée : phishing, fraude au président, vishing.	Réflexes, entraînement continu, procédures de vérification.
Usage malveillant interne	Abus délibéré de droits légitimes.	Moindre privilège, revue des accès, journalisation, RH/juridique.

~20 %

des violations notifiées à la CNIL en 2024 sont dues à une erreur humaine interne.
CNIL, Violations massives de données en 2024

68 %

des employés reconnaissent prendre sciemment des risques de sécurité (mots de passe, clics, partage d'identifiants).
Proofpoint, 2024 State of the Phish

L'écart connaissance / comportement

Savoir n'est pas faire. Une part importante des risques est prise en connaissance de cause, souvent par contrainte de productivité. La culture cyber ne consiste donc pas seulement à informer, mais à rendre le comportement sûr plus simple que le comportement risqué.

03 3. Panorama chiffré de la menace 2024-2026 (France + Europe)

Les grands rapports 2024-2026 convergent : la menace augmente en volume et en sophistication, le facteur humain reste la porte d'entrée dominante, et le coût des incidents demeure élevé. Voici la synthèse source par source.

Source	Indicateur clé	Enseignement
ANSSI — Panorama 2024	4 386 événements traités (+15 %)	Hausse continue, montée des attaques par rebond via tiers.
Cybermalveillance.gouv.fr 2024	~420 000 demandes (+49,9 %)	Hameçonnage = première menace côté PME/TPE et grand public.
ENISA — Threat Landscape 2025	Phishing = intrusion initiale n°1	Industrialisation via Phishing-as-a-Service et IA.
CESIN / OpinionWay 2025	40 % des entreprises touchées	Phishing/smishing/vishing = point d'entrée dans 55 % des cas.
IBM — Cost of a Data Breach 2025	4,44 M\$ coût moyen mondial	Phishing = vecteur initial le plus fréquent (16 %).

+15 % (4 386)

événements de sécurité traités par l'ANSSI en 2024, en hausse de 15 %.

ANSSI, Panorama de la cybermenace 2024

~420 000 / +49,9 %

demandes d'assistance reçues par Cybermalveillance.gouv.fr en 2024, l'hameçonnage restant la première menace.

Cybermalveillance.gouv.fr, Rapport d'activité 2024

La part croissante de l'IA offensive

Selon l'ENISA (Threat Landscape 2025), plus de 80 % des e-mails de phishing analysés récemment intègrent l'IA à un certain degré : rédaction sans fautes en quelques minutes, personnalisation de masse, deepfakes audio/vidéo pour la fraude au président, quishing (QR codes) et technique « ClickFix ». Le coût de production d'une attaque crédible s'effondre : la vigilance ne peut plus reposer sur la détection des « fautes d'orthographe ».

04 4. Vulgarisation : culture cyber vs sensibilisation ponctuelle

Deux notions sont souvent confondues. La sensibilisation ponctuelle est un événement : une session, une vidéo, un quiz annuel. Elle informe, mais son effet décroît en quelques semaines. La culture cyber est un état durable : des comportements partagés, des réflexes automatiques, une norme sociale interne où signaler un doute est valorisé et où la sécurité fait partie du « comment on travaille ici ».

1. Conformité — on fait parce qu'on doit (obligation, audit). Nécessaire mais insuffisant.
2. Sensibilisation — les personnes savent identifier les risques principaux.
3. Comportement — les personnes agissent correctement, même sous pression et sans supervision.
4. Culture — les bons comportements sont la norme, se transmettent entre pairs et survivent aux départs.

Le modèle de maturité (SANS)

Le SANS Security Awareness Report structure la maturité d'un programme sur plusieurs niveaux, du programme inexistant au programme « métrique » qui mesure son impact comportemental et l'améliore en continu. Situer sa maturité est le point de départ de tout plan crédible (voir section 13).

1,8 à 4,2 ETP

effectifs dédiés observés dans les programmes de sensibilisation les plus matures.

SANS Institute, 2024 Security Awareness Report

05 5. Ingénierie sociale et phishing décryptés

L'ingénierie sociale exploite des ressorts psychologiques universels, pas des failles techniques. Comprendre ces leviers aide à les désamorcer collectivement.

- Autorité — un message qui semble venir du dirigeant, d'un fournisseur clé ou de l'IT.
- Urgence — « à traiter dans l'heure », « votre compte sera bloqué » : couper la réflexion.
- Peur — menace de sanction, de perte, de honte.
- Réciprocité et sympathie — un service rendu, un ton amical, un contexte plausible.
- Preuve sociale — « tout le monde l'a déjà fait », faux fil de discussion interne.

Forme	Canal	Exemple typique
Phishing	E-mail de masse	Fausse facture, faux avis de livraison.
Spear-phishing	E-mail ciblé	Message personnalisé à un comptable nommément.
Smishing / Vishing	SMS / appel voix	Faux SMS bancaire, faux support technique au téléphone.
Quishing	QR code	QR code piégé sur affiche, e-mail ou faux parking.
Fraude au président	E-mail / voix / deepfake	Virement urgent et confidentiel « demandé par le dirigeant ».
ClickFix	Page web / e-mail	Instructions pour « réparer » un affichage, qui exécutent en fait du code.

>80 %

des e-mails de phishing récents utilisent l'IA à un certain degré, accélérant et industrialisant l'ingénierie sociale.

ENISA, Threat Landscape 2025

Anatomie d'un e-mail piégé

Signaux à enseigner : expéditeur affiché plausible mais domaine réel différent ; pression temporelle ; demande inhabituelle (changement d'IBAN, achat de cartes cadeaux) ; lien dont l'URL réelle diffère du texte ; pièce jointe inattendue ; rupture de canal (« ne m'appellez pas, répondez par mail »). Règle d'or à ancrer : pour toute demande financière ou de changement de coordonnées, vérification par un second canal connu, jamais celui fourni dans le message.

06 6. Cadre réglementaire et obligations

La sensibilisation n'est plus une bonne pratique optionnelle : plusieurs textes en font une obligation, avec une responsabilité qui remonte jusqu'aux dirigeants.

Texte	Ce qu'il impose (facteur humain)	Point de vigilance
NIS2 — Directive (UE) 2022/2555, art. 20	Responsabilité des organes de direction, formation obligatoire des dirigeants, encouragement à former tous les salariés.	Directive non transposée en droit français au 14/10/2026. Responsabilité personnelle possible ; sanctions pour l'entité.
RGPD — via la CNIL	Sécurité des données (art. 32), notification d'une violation sous 72 h (art. 33), information des personnes.	Erreur humaine = violation notifiable.
DORA (secteur financier)	Résilience opérationnelle numérique, formation et tests, gestion des risques liés aux tiers.	S'ajoute à NIS2 pour les entités financières.

5 629 / +20 %

notifications de violations reçues par la CNIL en 2024, en hausse de 20 % sur un an.
CNIL, Violations massives de données en 2024

Responsabilité personnelle des dirigeants (NIS2)

L'article 20 de la directive NIS2 place la cybersécurité au niveau de l'organe de direction : approbation des mesures de gestion des risques, supervision, et obligation de suivre une formation. Il encourage explicitement à proposer une formation similaire aux salariés. La culture cyber devient ainsi un sujet de gouvernance, pas seulement d'IT. La directive n'est pas transposée en droit français au 14/10/2026 : ces obligations ne sont pas encore opposables en France.

Positionnement Sedona

Sedona.AI évalue votre exposition et les signaux de conformité (cartographie, audit, OSINT) pour vous aider à anticiper. Sedona ne certifie pas, ne garantit pas la conformité et n'est pas un organisme de certification ni un prestataire de réponse à incident.

07 7. Le sponsor top-management : sans direction, pas de culture

Une culture ne se décrète pas par une note de service : elle s'incarne par l'exemple. Si la direction ne priorise pas visiblement la cybersécurité, aucune campagne ne compensera ce signal. Le sponsor top-management est le facteur de succès le plus discriminant d'un programme de sensibilisation.

- ☐ Allouer un budget et du temps dédiés (au moins un référent identifié).
- ☐ Participer personnellement aux formations et aux simulations, sans exemption.
- ☐ Communiquer régulièrement en interne sur l'importance du sujet, en ton positif.
- ☐ Intégrer des objectifs cyber dans les revues d'activité et les objectifs des managers.
- ☐ Arbitrer les risques explicitement quand un choix oppose sécurité et productivité.
- ☐ Valoriser publiquement les signalements, y compris les faux positifs.

Effet miroir

Quand un dirigeant signale lui-même un e-mail douteux et le raconte, il légitime le comportement pour toute l'organisation. Quand il exige d'être exempté de MFA « parce qu'il est pressé », il détruit des mois de pédagogie.

08 8. Levier 1 — Formation continue et micro-learning

La formation annuelle unique est le principal anti-pattern du secteur : dense, oubliée en quelques semaines, déconnectée du quotidien. La recherche en apprentissage plaide pour la répétition espacée : des séquences courtes, régulières, contextualisées et différenciées par métier valent mieux qu'un long module annuel.

1 Micro-modules réguliers

5 à 10 minutes, mensuels ou trimestriels, un thème à la fois (phishing, mots de passe, données, mobilité).

2 Contextualisation par métier

La comptabilité voit la fraude au virement ; les RH, le phishing de candidature ; les commerciaux, le wifi public et le vol d'appareil.

3 Nudges au fil de l'eau

Rappels courts au bon moment (bannière e-mail externe, message avant un virement) plutôt qu'un cours théorique.

4 Renforcement à l'erreur

Quand quelqu'un clique sur une simulation, proposer immédiatement une micro-formation ciblée de 60 secondes, sans humiliation.

Honnêteté sur l'efficacité

Les éditeurs annoncent des baisses spectaculaires du taux de vulnérabilité (par ex. de ~33 % à ~4 % après 12 mois de formation continue, KnowBe4 — source éditeur à nuancer). Des études indépendantes sont plus prudentes : l'effet dépend fortement de la qualité et de la régularité du dispositif. Visez la constance et la mesure, pas la promesse chiffrée.

~33 % → ~4 %

taux d'employés vulnérables au phishing avant formation, ramené après 12 mois de formation continue (source éditeur, à nuancer).

KnowBe4, Phishing by Industry Benchmarking 2024

09 9. Levier 2 — Simulations de phishing : bonnes pratiques et pièges

Les simulations de phishing ont une double vertu : mesurer un comportement réel et entraîner le réflexe de signalement. Mais mal conçues, elles peuvent être inutiles, voire contre-productives — dégradant la confiance sans réduire le risque.

- ☐ Former au moment de l'erreur : la page de « débriefing » après un clic est le meilleur moment pédagogique.
- ☐ Ne jamais utiliser d'appât humiliant ou cruel (fausse prime, faux licenciement, deuil, santé).
- ☐ Mesurer le taux ET la rapidité de signalement, pas seulement le taux de clic.
- ☐ Prévenir en amont de l'existence d'un programme de simulation (transparence sur le principe, pas sur le calendrier).
- ☐ Adapter la difficulté progressivement et par population.
- ☐ Ne jamais sanctionner un clic : sanctionner tue le signalement (voir section 16).

28 minutes

temps médian avant qu'un e-mail de phishing soit signalé, laissant une large fenêtre à l'attaquant.

Verizon, 2025 Data Breach Investigations Report

Ce que la recherche récente nuance

Plusieurs travaux indépendants montrent que les simulations de phishing, prises isolément, produisent des gains parfois marginaux sur le taux de clic à long terme, et que des dispositifs punitifs peuvent réduire la propension à signaler. La simulation n'est pas une fin : c'est un outil de mesure et d'entraînement, qui ne vaut que couplé à une formation bienveillante et à une culture du signalement. Objectif prioritaire : faire chuter le délai de signalement bien en dessous de 28 minutes.

10. Levier 3 — Onboarding et parcours par rôle

La cyber doit devenir un réflexe dès le premier jour. Un nouvel arrivant non sensibilisé, doté d'accès et pressé de « bien faire », est une cible idéale pour la fraude au président ou le phishing de bienvenue. L'onboarding est un moment à fort levier culturel.

1 Jour 1

Module d'accueil cyber (30-45 min), remise et signature de la charte informatique, activation du MFA, mise en place du gestionnaire de mots de passe.

2 Semaine 1

Accès selon le moindre privilège, présentation du canal de signalement en 1 clic, focus sur les 3 arnaques les plus fréquentes dans l'entreprise.

3 Jour 30

Micro-quiz de consolidation, première simulation bienveillante, entretien avec le référent cyber ou le manager pour lever les doutes.

Population à risque	Menace prioritaire	Contenu spécifique
Comptabilité / Finance	Fraude au virement, faux IBAN	Procédure de double validation, vérification second canal.
RH	Phishing de candidature, fuite de données	Pièces jointes, données personnelles, RGPD.
Dirigeants / Assistants	Fraude au président, deepfake	Vérification d'identité, confidentialité, exposition publique.
IT / Admins	Vol d'identifiants à privilèges	MFA FIDO2, comptes séparés, gestion des secrets.
Commerciaux nomades	Wifi public, vol/perte d'appareil	VPN, chiffrement, verrouillage, écran de confidentialité.

11. Levier 4 — Hygiène des accès : mots de passe, MFA, gestion des droits

La technique et l'humain se rejoignent ici. Un seul contrôle change radicalement l'équation du risque : l'authentification multifacteur. Elle transforme un mot de passe volé en incident non exploitable.

>99,2 %

des attaques de compromission de compte sont bloquées par l'authentification multifacteur (MFA).

Microsoft / étude de mesure (arXiv 2023)

- Généraliser le MFA, idéalement résistant au phishing (FIDO2 / clés physiques ou passkeys) sur les accès sensibles.
- Déployer un gestionnaire de mots de passe : il rend possible des mots de passe uniques et longs sans effort de mémorisation.
- Appliquer le moindre privilège : chacun n'a que les accès nécessaires à son rôle.
- Instaurer une revue périodique des accès et un processus strict de retrait à chaque départ.
- Privilégier les phrases de passe longues plutôt que des règles de complexité arbitraires (recommandations ANSSI / NIST).

Politique de mot de passe minimale

Phrase de passe longue (au moins 12-16 caractères) ; unique par service (via gestionnaire) ; jamais de rotation forcée systématique sans motif ; MFA obligatoire sur messagerie, VPN, outils financiers et comptes administrateurs ; blocage des mots de passe compromis connus. Le MFA n'est pas une option pour les comptes à privilèges.

12. Levier 5 — Télétravail, BYOD et mobilité

Le travail hybride a dissous le périmètre : réseaux non maîtrisés, appareils personnels, déplacements. Les règles doivent être pragmatiques pour être suivies.

- Accès conditionnel / VPN pour les ressources internes ; éviter l'exposition directe de services.
- Gestion des appareils (MDM) et chiffrement du disque sur tout poste mobile.
- Verrouillage automatique de session et écran de confidentialité en déplacement.
- Wifi public : proscrire les opérations sensibles sans VPN ; méfiance envers les bornes de recharge USB inconnues.
- Séparation vie pro / perso claire, surtout en BYOD (conteneurisation, comptes distincts).

Charte télétravail — clauses cyber essentielles

Équipements autorisés et interdits ; obligation de MFA et de mises à jour ; interdiction de stockage local non chiffré de données sensibles ; conduite à tenir en cas de perte/vol (signalement immédiat) ; règles sur le wifi et les tiers ; confidentialité des écrans en espace public. À intégrer à la charte informatique générale (section 21).

13. Méthode — Étape 1 : état des lieux initial et baseline

On ne pilote que ce qu'on mesure. Avant tout plan, établissez un point zéro objectif : sans baseline, impossible de démontrer un progrès ni de prioriser.

1 Évaluer la maturité

Positionner le programme actuel sur le modèle SANS (de inexistant à métrique). Identifier qui porte le sujet et avec quels moyens.

2 Mesurer un point zéro

Simulation de phishing de référence (taux de clic ET de signalement), enquête de perception anonyme, revue rapide des accès et du MFA.

3 Cartographier l'exposition

Recenser les populations et scénarios à risque, et l'exposition externe (données publiques, e-mails exposés, surface d'attaque) via un audit/OSINT.

4 Prioriser

Croiser impact et effort pour définir 3 à 5 actions à fort levier immédiat (souvent MFA, gestionnaire, signalement, charte).

40 %

des entreprises françaises déclarent avoir subi au moins une cyberattaque significative en 2025.

CESIN, Baromètre de la cybersécurité des entreprises 2025 (11e édition)

Rôle de Sedona à cette étape

Sedona.AI intervient en amont sur la cartographie d'exposition et l'audit/OSINT : identifier ce qu'un attaquant voit de votre organisation (domaines, e-mails exposés, services accessibles, signaux de risque). Cet éclairage nourrit l'état des lieux et priorise les scénarios de sensibilisation. Sedona Radar évalue cette exposition ; il ne certifie pas et ne rend pas conforme.

14 14. Méthode — Étape 2 : construire le plan de sensibilisation sur 12 mois

Un plan annuel structure objectifs, publics, thèmes, formats, cadence, budget et gouvernance. L'enjeu est la régularité : mieux vaut un rythme mensuel léger qu'un grand événement unique.

Période	Thème	Format
Mois 1-2	Lancement + phishing & signalement	Kick-off direction, micro-module, baseline.
Mois 3	Mots de passe & MFA	Nudge + déploiement gestionnaire.
Mois 4	Données personnelles & RGPD	Micro-module + quiz.
Mois 5	Simulation de phishing n°1	Simulation + débriefing bienveillant.
Mois 6	Mobilité, télétravail, BYOD	Micro-module ciblé nomades.
Mois 7-8	Ingénierie sociale & fraude au président	Atelier métiers finance/direction.
Mois 9	Simulation n°2 + IA offensive (deepfakes, quishing)	Simulation + sensibilisation IA.
Mois 10	Sauvegardes & réflexes en cas d'incident	Exercice de signalement.
Mois 11	Campagne ambassadeurs / gamification	Défi d'équipe positif.
Mois 12	Bilan annuel & re-baseline	Reporting direction, ajustement du plan.

Modèle réutilisable et ressources gratuites

Le Kit de sensibilisation de Cybermalveillance.gouv.fr (9 thématiques : guides, fiches, mémos, affiches, vidéos, quiz) est réutilisable sous licence ouverte Etalab 2.0. Il permet de bâtir un plan complet sans budget de contenu. Le NIST Cybersecurity Framework 2.0 fournit un cadre pour aligner le programme sur un standard reconnu.

15 15. Méthode — Étape 3 : campagnes, KPIs et mesure

Le taux de clic seul est un mauvais indicateur : il mesure l'échec, pas le réflexe. Un tableau de bord utile distingue métriques de comportement (ce que font les gens) et métriques de culture (ce qu'ils pensent et ressentent).

Indicateur	Ce qu'il mesure	Objectif
Taux de signalement	Réflexe de remonter un e-mail douteux	En hausse (l'indicateur le plus important).
Délai médian de signalement	Rapidité de la première alerte	Le plus bas possible (bien sous 28 min).
Taux de clic sur simulation	Exposition résiduelle	En baisse progressive, sans obsession.
Taux de récurrence	Ancrage de l'apprentissage	En baisse.
Participation aux formations	Couverture réelle du programme	Élevée et stable.
Perception (enquête)	Sécurité psychologique, culture	En amélioration.

55 %

des cyberattaques significatives en France ont pour point d'entrée le phishing/spear-phishing/smishing/vishing.

CESIN, Baromètre de la cybersécurité des entreprises 2025 (11e édition)

Reporting à la direction

Rythme trimestriel, une page : tendance du taux et du délai de signalement, couverture des formations, incidents évités grâce au signalement, points d'attention et décisions demandées. Relier ces KPIs à la supervision de l'organe de direction que prévoit NIS2 (art. 20).

16 16. Méthode — Étape 4 : culture du signalement sans blâme (no-blame)

C'est le cœur de la culture cyber. Chaque minute compte : plus une alerte remonte vite, plus la réponse est efficace. Or la culpabilisation produit l'inverse : la personne qui a cliqué a peur, se tait, et l'attaquant gagne du temps. Une culture du signalement sans blâme (no-blame) traite l'erreur comme un signal précieux, pas comme une faute.

21 s → 28 min

de 21 secondes pour cliquer sur un lien piégé à 28 minutes avant le premier signalement : l'attaquant dispose d'une fenêtre d'environ 28 minutes que seule une remontée rapide referme.

Verizon, 2025 Data Breach Investigations Report

- Rendre le signalement trivial : un bouton « signaler » dans la messagerie, un canal unique connu de tous.
- Remercier systématiquement, y compris pour les faux positifs — un faux positif vaut mieux qu'un silence.
- Ne jamais sanctionner un clic ; traiter la récidive par de l'accompagnement, pas par la punition.
- Communiquer les « saves » : « grâce à un signalement rapide, une attaque a été stoppée » (anonymisé, positif).
- Séparer clairement erreur honnête et malveillance délibérée : seule la seconde relève de la sanction.

Sécurité psychologique = temps de détection

Le vrai KPI de maturité n'est pas « combien de personnes ont cliqué » mais « en combien de temps la première alerte est-elle remontée ». Une culture no-blame fait chuter ce délai — c'est là que se gagne la réduction de l'impact.

17 17. Ancrage durable : nudges, gamification, ambassadeurs

Le one-shot ne crée pas d'habitude. L'ancrage repose sur la répétition espacée, l'intégration aux processus métiers et une animation qui vit au-delà de l'équipe sécurité.

- Réseau d'ambassadeurs / référents cyber par service : relais de proximité, remontée du terrain.
- Gamification maîtrisée : défis d'équipe positifs, reconnaissance des bons réflexes (pas de name-and-shame).
- Rappels contextuels (nudges) au moment utile plutôt que formations décontextualisées.
- Rituels d'équipe : point cyber de 5 minutes en réunion, « minute sécurité » mensuelle.
- Communication interne récurrente et variée pour éviter l'usure du message.

Comment éviter la lassitude

Varier formats et tons ; rester bref ; célébrer plutôt que menacer ; relier chaque message à un risque concret et actuel (une arnaque en cours dans le secteur) ; ne pas sur-solliciter (la fatigue d'alerte est réelle). Une culture s'entretient comme une hygiène, pas comme une campagne de choc.

18 18. Les erreurs fréquentes qui sabotent la démarche

La plupart des échecs suivent des schémas connus. Les repérer, c'est éviter de gaspiller budget et crédibilité.

Anti-pattern	Pourquoi ça échoue	Correctif
Formation annuelle unique	Oubliée en quelques semaines.	Micro-learning régulier et espacé.
Ton anxigène ou culpabilisant	Bloque le signalement, génère du rejet.	Ton positif, valorisation des bons réflexes.
Simulations punitives	Détruit la confiance, cache les incidents.	Débriefing bienveillant, aucune sanction du clic.
Contenu générique	Ne parle pas au métier de chacun.	Contextualisation par population à risque.
Absence de mesure	Impossible de prouver l'impact ni d'ajuster.	Baseline + KPIs de signalement.
Pas de sponsor direction	Le message n'est pas légitime.	Engagement visible de la direction (NIS2).
Oublier tiers et prestataires	La chaîne d'approvisionnement est un vecteur majeur.	Étendre exigences et sensibilisation aux tiers.

37 %

part des TPE/PME/ETI parmi les victimes de rançongiciel signalées à l'ANSSI en 2024.
ANSSI, Panorama de la cybermenace 2024

19. Spécificités PME/ETI : faire beaucoup avec peu

Les PME et ETI sont massivement visées, souvent sans RSSI dédié, avec un budget et un temps limités. L'ENISA le confirme : sous-priorisation de la cyber, manque de moyens et de personnel. La réponse n'est pas de tout faire, mais de faire d'abord ce qui compte le plus.

☐ MFA activé partout où c'est possible (messagerie, VPN, outils financiers, admin).

☐ Gestionnaire de mots de passe déployé et adopté.

☐ Canal de signalement en 1 clic et culture no-blame.

☐ Kit gratuit Cybermalveillance.gouv.fr comme socle de contenu.

☐ Sauvegardes régulières, testées, dont une copie hors ligne.

- ☐ Un référent cyber identifié (même à temps partiel) et un sponsor direction.

Programme cyber-culture à budget zéro

Contenus : kit Cybermalveillance (licence ouverte) + cadre NIST 2.0. Cadence : une « minute sécurité » mensuelle en réunion d'équipe. Mesure : une simulation de référence par semestre, suivi du délai de signalement. Gouvernance : le dirigeant ouvre chaque trimestre par un message cyber. Coût principal : du temps et de la constance, pas de la licence logicielle.

4,44 M\$

coût moyen mondial d'une violation de données en 2025 — un rappel que la prévention reste bien moins coûteuse que l'incident.

IBM, Cost of a Data Breach Report 2025

20. Checklist opérationnelle 30 / 60 / 90 jours

Un plan d'attaque concret par jalons, décliné par rôle. À cocher au fur et à mesure.

- ☐ J+30 — Activer le MFA sur les comptes critiques ; diffuser et faire signer la charte ; mettre en place le bouton de signalement ; nommer un référent cyber et obtenir l'engagement écrit du dirigeant.
- ☐ J+60 — Réaliser la baseline (simulation de référence + enquête de perception) ; déployer le gestionnaire de mots de passe ; publier le premier micro-module ; tenir la première « minute sécurité ».
- ☐ J+90 — Lancer la première campagne complète ; instaurer le tableau de bord KPIs (signalement en priorité) ; faire la première revue trimestrielle avec la direction ; planifier les 12 mois.

Rôle	Priorité immédiate	À 90 jours
Dirigeant	Sponsoriser, activer son propre MFA, communiquer.	Revue trimestrielle, arbitrages de risque documentés.
DRH	Intégrer cyber à l'onboarding, diffuser la charte.	Parcours par rôle en place, référents identifiés.
DSI / RSSI	MFA, gestionnaire, canal de signalement.	Baseline, KPIs, première campagne mesurée.

21. Modèles prêts à l'emploi

Cinq livrables à adapter et réutiliser pour démarrer sans repartir de zéro.

1. Charte informatique / de sensibilisation — usages autorisés, MFA, signalement, télétravail, conséquences ; signée à l'onboarding.
2. Trame de plan de sensibilisation 12 mois — objectifs, publics, thèmes, formats, cadence, budget, KPIs (voir section 14).
3. Politique de mot de passe / MFA — phrases de passe, unicité, MFA obligatoire sur les accès sensibles (voir section 11).
4. Fiche de signalement d'incident — quoi signaler, comment, à qui, sous quel délai ; ton no-blame explicite.
5. Tableau de bord KPIs — taux et délai de signalement, clic, récidence, participation, perception (voir section 15).

Ressources ouvertes à mobiliser

Kit de sensibilisation Cybermalveillance.gouv.fr (licence Etalab 2.0, réutilisable et modifiable) pour les contenus ; NIST Cybersecurity Framework 2.0 pour structurer et aligner le programme sur un standard reconnu. Ces ressources évitent de payer pour du contenu générique.

22. Où s'adresser, anticiper et retours d'expérience

Aucune organisation n'est seule. En France et en Europe, des ressources officielles couvrent la prévention, l'assistance et la réponse.

- ANSSI / cyber.gouv.fr — doctrine, guides, panorama de la menace, référentiels.
- Cybermalveillance.gouv.fr — assistance PME/TPE, kit de sensibilisation, dispositif 17Cyber.
- CNIL — RGPD, notification de violation sous 72 h, guides sécurité.
- ENISA — panorama européen des menaces et recommandations PME.
- CERT sectoriels et prestataires de réponse à incident pour la gestion de crise.

Scénario	Ce qui a manqué (culture)	Enseignement
Fraude au président	Aucune procédure de vérification par second canal ; pression hiérarchique non contestable.	Ancrer la double validation des virements, non négociable même pour la direction.
Phishing rédigé par IA	Vigilance basée sur les « fautes d'orthographe » ; e-mail parfait.	Déplacer le réflexe vers la vérification de l'action demandée, pas la forme.
PME rançonnée après clic	Signalement tardif, peur de la sanction ; sauvegardes non testées.	Culture no-blame pour détecter tôt + sauvegardes hors ligne testées.

Le rôle de Sedona.AI, honnêtement

Sedona.AI intervient en amont : Sedona Radar analyse ce que votre domaine expose sur Internet ; en complément, un audit OSINT des dirigeants, des formations de sensibilisation et des simulations de phishing. Sedona Radar ne certifie rien, ne garantit pas la conformité et ne se substitue ni à un organisme de certification ni à un prestataire de réponse à incident. La culture, elle, reste l'œuvre de vos équipes et de votre direction ; ce guide est là pour l'outiller.

§ Sources

1. Verizon — 2025 Data Breach Investigations Report (DBIR) — <https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf>
2. ENISA — Threat Landscape 2025 — https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf
3. ENISA — Cybersecurity for SMEs: Challenges and Recommendations — <https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes>
4. IBM — Cost of a Data Breach Report 2025 (analyse X-Force) — <https://www.ibm.com/think/x-force/2025-cost-of-a-data-breach-navigating-ai>
5. IBM — Cost of a Data Breach (page rapport) — <https://www.ibm.com/reports/data-breach>
6. CNIL — Violations massives de données en 2024 : enseignements et mesures — <https://www.cnil.fr/fr/violations-massives-de-donnees-en-2024-quels-sont-les-principaux-enseignements-mesures-a-prendre>
7. CNIL — Violations de données personnelles : bilan de 5 années de RGPD — <https://www.cnil.fr/fr/violations-de-donnees-personnelles-bilan-de-5-annees-de-rgpd>
8. Cybermalveillance.gouv.fr — Rapport d'activité et état de la menace 2024 — https://www.cybermalveillance.gouv.fr/medias/2025/03/250327_RA_2024_SCREEN.pdf
9. Cybermalveillance.gouv.fr — Kit de sensibilisation (licence ouverte) — <https://www.cybermalveillance.gouv.fr/tous-nos-contenus/kit-de-sensibilisation>
10. ANSSI — Panorama de la cybermenace 2024 — <https://cyber.gouv.fr/actualites/panorama-de-la-cybermenace-2024-mobilisation-et-vigilance-face-aux-attaquants/>
11. CERT-FR / ANSSI — Panorama de la cybermenace 2024 (PDF) — <https://www.cert.ssi.gouv.fr/uploads/CERTFR-2025-CTI-003.pdf>
12. EUR-Lex — Directive (UE) 2022/2555 (NIS2), article 20 Gouvernance — <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>
13. Microsoft Security — MFA bloque >99 % des compromissions de compte — <https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/>
14. arXiv / Microsoft — How effective is MFA at deterring cyberattacks? — <https://arxiv.org/pdf/2305.00945>
15. SANS Institute — 2024 Security Awareness Report — <https://www.sans.org/security-awareness-training/resources/reports/sar/>
16. Proofpoint — 2024 State of the Phish — <https://www.proofpoint.com/us/resources/threat-reports/state-of-phish>
17. CESIN — Baromètre de la cybersécurité des entreprises (11e édition, 2025) — <https://cesin.fr/>
18. OpinionWay — Baromètre de la cybersécurité des entreprises pour le CESIN — <https://www.opinion-way.com/fr/publications/barometre-cybersecurite-entreprises-vague10-2025-19011/>
19. NIST — Cybersecurity Framework 2.0 — <https://www.nist.gov/cyberframework>
20. KnowBe4 — Phishing by Industry Benchmarking Report 2024 — <https://www.knowbe4.com/press/knowbe4-report-reveals-security-training-reduces-global-phishing-click-rates-by-86>

Passez de la lecture à l'action : sensibilisez vos équipes

Sedona forme vos équipes à la cybersécurité, sur site ou à distance ; la formation peut se compléter d'une simulation de phishing suivie d'un débrief collectif, sans sanction. Les tarifs sont sur les pages Formation et Services. Pour voir d'abord ce que votre domaine expose sur Internet, Sedona Radar offre un premier scan gratuit.

[Voir les formations](#)

sedona-ai.com/formation