

LIVRE BLANC · DÉCISIONS 2027

Piloter la cybersécurité et les usages de l'IA pour 2027

Cadrer les risques organiser une première sécurisation et préparer les projets complexes

POUR DÉCIDER

Préparer les bons arbitrages

Une démarche cyber doit permettre au dirigeant de décider ce qui protège son activité, qui doit agir et quelles preuves permettront de suivre l'avancement. Les outils sont une partie de la réponse. La responsabilité, les accès, la continuité, les prestataires et les usages de l'IA doivent également être organisés.

Ce livre blanc présente le rôle qu'un cabinet de stratégie appliquée comme 17 SECONDES peut proposer : cadrage, audit de préparation, organisation d'une première sécurisation, assistance au choix d'outils et maîtrise d'ouvrage de projets conduits avec les spécialistes adaptés. Le périmètre de chaque mission, les compétences nécessaires et les autorisations sont définis avant intervention.

Les méthodes de travail proposées ne constituent ni un audit certifié, ni une qualification PASSI, ni une garantie d'absence d'incident. Aucun test intrusif ou changement technique n'est engagé sur la seule base de ce guide. Notre recommandation est de relier une première action vérifiable aux activités essentielles de l'entreprise, puis de traiter les sujets complexes avec les experts requis.

À utiliser en comité de direction

Les fiches en fin de document permettent de transformer cette lecture en décisions : besoin, preuve, responsable, moyens et prochaine étape.

PARCOURS DE LECTURE

Huit questions pour avancer

01 Relier la sécurité aux activités essentielles

La priorité cyber se définit à partir de l'activité et de ses dépendances.

02 Définir un audit de préparation vérifiable

La valeur de l'audit tient à ses preuves et à ses limites annoncées.

03 Organiser une première sécurisation

Une mesure est mise en œuvre lorsqu'elle a un responsable et une preuve de fonctionnement.

04 Préparer la continuité et la réponse à un incident

La préparation cyber doit inclure le fonctionnement de secours et les responsabilités en cas d'incident.

05 Utiliser l'IA pour assister l'audit

L'IA assiste l'organisation des preuves ; elle ne remplace pas leur vérification.

06 Sécuriser les usages de l'IA

Les accès et les actions autorisées d'un système d'IA doivent être maîtrisés et vérifiables.

07 Choisir les experts et conduire l'AMO

L'AMO relie les besoins de la direction aux travaux des spécialistes et aux preuves de recette.

08 Construire une feuille de route pour 2027

Le programme cyber devient pilotable lorsque chaque étape peut être décidée et vérifiée.

MÉTHODE · 01

Relier la sécurité aux activités essentielles

Commencez par les activités dont l'arrêt aurait une conséquence importante pour l'organisation. Décrivez ce qui doit continuer : servir les clients, produire, facturer, accéder aux documents ou coordonner les équipes. La première discussion porte sur l'activité et les dépendances qui permettent de la réaliser.

Identifiez pour chacune les outils, les données, les personnes et les prestataires nécessaires. Une cartographie de travail n'a pas besoin d'être exhaustive au premier jour ; elle doit rendre visibles les dépendances critiques et les zones inconnues. Les acteurs métier doivent pouvoir la relire et confirmer son contenu.

Le guide de pilotage de [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) replace la cybersécurité au niveau de la direction et recommande le recours à des prestataires spécialisés pour les systèmes critiques [1]. Cette approche aide à distinguer ce que la gouvernance peut décider de ce qui nécessite une expertise technique spécifique.

Conservez les conséquences décrites par l'entreprise et les hypothèses à vérifier. Évitez un montant de risque présenté comme certain lorsque le scénario, la fréquence ou les coûts sont mal établis. Le premier livrable est une lecture partagée des activités, des dépendances et des décisions nécessaires.

À RETENIR

La priorité cyber se définit à partir de l'activité et de ses dépendances.

MÉTHODE · 02

Définir un audit de préparation vérifiable

Un audit de préparation peut réunir des entretiens, la lecture des documents existants et des vérifications non intrusives autorisées. Son objectif est de rendre les décisions possibles : ce qui est documenté, ce qui est établi, ce qui manque et ce qui doit être contrôlé par un spécialiste. Son périmètre reste explicite.

Définissez les systèmes concernés, les sources consultables, les interlocuteurs et les livrables. Précisez les accès autorisés et les éléments exclus. Si un outil est utilisé pour collecter des informations, indiquez ce qu'il observe et les actions qu'il ne peut pas déclencher sans nouvel accord.

Chaque constat porte une preuve, une date, une conséquence et une limite. La déclaration d'un prestataire n'est pas identique à une configuration observée. Un document ancien ne prouve pas l'état actuel du dispositif. Une information absente ne doit pas être transformée en conformité supposée.

Présentez les résultats sans faux score de sécurité. Une synthèse peut distinguer les sujets établis, à vérifier et à traiter. Les constats techniques qui exigent un test d'intrusion, une investigation ou une évaluation spécialisée doivent être transmis à un expert disposant du périmètre et des autorisations adaptés.

À RETENIR

La valeur de l'audit tient à ses preuves et à ses limites annoncées.

MÉTHODE · 03

Organiser une première sécurisation

Les mesures d'hygiène informatique constituent un socle à examiner dans le contexte de l'entreprise. Le guide de l'ANSSI regroupe 42 mesures portant sur la connaissance du système, les accès, la protection, l'administration et les autres dimensions de la sécurité [2]. Il n'établit pas qu'une organisation soit protégée parce qu'elle possède une liste de contrôle.

Choisissez un premier périmètre avec le responsable informatique ou le prestataire. Pour chaque action, précisez la situation de départ, le responsable de la mise en œuvre et la preuve attendue. Une action sur les comptes, les sauvegardes ou les équipements doit être préparée avec les personnes qui assurent leur fonctionnement.

La sécurisation d'un site, par exemple, peut nécessiter la maîtrise des accès administrateurs, la mise à jour des composants et une sauvegarde dont la restauration est testée [3]. Le cabinet peut aider à organiser les décisions et les vérifications ; le changement technique est réalisé par les intervenants compétents dans le périmètre accepté.

Conservez une trace de la modification, de la vérification et des conséquences constatées. Un changement qui perturbe le service peut demander un ajustement. La première sécurisation doit ainsi produire un résultat observé et une documentation utilisable, pas seulement un engagement de principe.

À RETENIR

Une mesure est mise en œuvre lorsqu'elle a un responsable et une preuve de fonctionnement.

MÉTHODE · 04

Préparer la continuité et la réponse à un incident

La préparation doit aussi envisager une indisponibilité. Identifiez les décisions à prendre, les personnes à joindre et les activités qui peuvent continuer autrement. Les coordonnées et les documents utiles doivent rester accessibles dans une situation où certains outils de l'entreprise sont indisponibles.

Distinguez la sauvegarde d'une donnée de la capacité à reprendre un service. Demandez ce qui a été restauré, quand et dans quelles conditions. Les objectifs de reprise doivent être définis par l'entreprise avec ses responsables métier et techniques. Un exercice limité peut révéler des dépendances qui n'étaient pas visibles dans les documents.

Le NIST CSF 2.0 propose une lecture du risque autour de six fonctions : gouverner, identifier, protéger, détecter, répondre et rétablir [4]. Ce cadre peut aider le comité de direction à s'assurer que son programme ne se concentre pas uniquement sur l'achat de protections.

Pour une situation réelle, la décision d'intervention revient aux responsables et aux spécialistes habilités pour le périmètre. Le cabinet peut contribuer à la coordination, à la documentation et au suivi des décisions. La gestion technique d'un incident ou l'analyse forensique doit être confiée aux experts appropriés.

À RETENIR

La préparation cyber doit inclure le fonctionnement de secours et les responsabilités en cas d'incident.

MÉTHODE · 05

Utiliser l'IA pour assister l'audit

L'IA peut être envisagée pour organiser des documents, préparer une synthèse ou rapprocher un constat d'une grille de travail. Ces usages doivent rester reliés à des sources consultables. Le résultat proposé est relu et validé par la personne responsable avant d'entrer dans une conclusion de mission.

Le périmètre de données est décidé avant l'utilisation. Un document de sécurité peut contenir des informations sensibles sur les accès, les systèmes ou les personnes. Les conditions d'hébergement, de conservation, de réutilisation et d'accès doivent être examinées. Les recommandations de la CNIL aident à instruire les conditions d'usage d'une IA générative [5].

Conservez le lien entre chaque sortie et les éléments qui la soutiennent. Une formulation plausible ne démontre pas l'existence d'une configuration ou d'une faille. Les informations contradictoires restent visibles. Une conclusion technique ne doit pas être automatisée sur la seule base d'une synthèse de documents.

Évaluez l'assistant sur des cas connus avant de l'intégrer au travail. Mesurez la qualité de restitution, les omissions, les erreurs et le temps de contrôle. L'outil doit pouvoir être écarté lorsque son apport ne compense pas la supervision nécessaire. Son usage ne crée pas une compétence ou une qualification que l'intervenant ne possède pas.

À RETENIR

L'IA assiste l'organisation des preuves ; elle ne remplace pas leur vérification.

MÉTHODE · 06

Sécuriser les usages de l'IA

Un système d'IA doit être étudié comme une architecture avec des entrées, des composants, des accès et des sorties. Les recommandations ANSSI sur l'IA générative portent notamment sur les conditions de sécurisation de cette architecture [6]. Le choix d'un modèle ne suffit donc pas à établir la sécurité de son intégration.

Décrivez ce que le système peut lire et ce qu'il peut faire. Pour un premier usage, limitez les actions et conservez une validation humaine lorsqu'une sortie déclenche une modification, un envoi ou une décision importante. Les droits de l'assistant doivent correspondre au périmètre réellement accepté.

Vérifiez le traitement d'une entrée inattendue ou d'une instruction présente dans un document. Le système doit conserver les règles de son usage et les limites de ses accès. Les contrôles nécessaires dépendent de la conception ; un spécialiste peut devoir examiner les mécanismes avant une mise en service sensible.

Organisez enfin les versions, les journaux utiles et les changements de sources. Un connecteur ajouté peut modifier le risque. Les responsables doivent pouvoir savoir ce qui a changé, qui l'a autorisé et quelles vérifications ont été réalisées. La sécurité d'un usage d'IA se maintient avec son fonctionnement.

À RETENIR

Les accès et les actions autorisées d'un système d'IA doivent être maîtrisés et vérifiables.

MÉTHODE · 07

Choisir les experts et conduire l'AMO

Les projets cyber complexes demandent des compétences qui doivent être identifiées avant l'engagement. Préparez un cahier des charges qui explique les systèmes, les objectifs, les livrables et les contraintes. Le cabinet peut assurer l'assistance à maîtrise d'ouvrage : cadrer le besoin, organiser la comparaison et aider l'entreprise à décider.

Examinez les preuves de compétence correspondant à la mission, les références utilisables et les conditions d'intervention. Une qualification ou une certification éventuelle doit être vérifiée pour le prestataire et le périmètre concernés. Aucune qualité détenue par un partenaire ne se transfère automatiquement au cabinet qui coordonne le projet.

Pendant l'exécution, suivez les dépendances, les demandes de changement et les livrables. Le responsable technique doit pouvoir expliquer les conclusions et les recommandations. Les écarts au périmètre, les actions complémentaires et les coûts sont soumis aux décisions prévues dans le projet.

La recette distingue ce qui a été remis de ce qui a été testé et accepté. Demandez les documents utiles à l'exploitation, la liste des sujets restant ouverts et les responsabilités de maintien. La mission se termine avec une situation compréhensible pour l'entreprise et une prochaine décision explicite.

À RETENIR

L'AMO relie les besoins de la direction aux travaux des spécialistes et aux preuves de recette.

MÉTHODE · 08

Construire une feuille de route pour 2027

Rassemblez les actions dans une feuille de route dont chaque ligne précise le sujet, la conséquence, le responsable, la dépendance, le coût à instruire et la preuve de réussite. Classez les actions selon leur utilité et les conditions de réalisation. Évitez une longue liste d'outils qui ne dit pas ce que l'entreprise doit décider.

Distinguez les premières mesures, les vérifications complémentaires et les projets nécessitant un expert. La priorité peut changer lorsque de nouvelles preuves apparaissent. Le programme doit conserver ce changement et sa raison, avec une version consultable par les responsables.

Pour le budget, séparez cadrage, réalisation, abonnements, fonctionnement et temps interne. Les montants inconnus restent à chiffrer. Une solution présentée comme gratuite peut demander une administration importante. Les conditions de sortie, la remise des accès et l'export des données sont examinés avant le choix.

Le comité de direction reçoit une synthèse courte : ce qui a été vérifié, ce qui a été amélioré, les sujets ouverts et les décisions attendues. Les pièces de preuve restent accessibles à un niveau approprié de confidentialité. Cette organisation permet d'avancer sur des faits sans promettre une sécurité absolue.

À RETENIR

Le programme cyber devient pilotable lorsque chaque étape peut être décidée et vérifiée.

OUTIL DE TRAVAIL

Fiche de constat à compléter

À compléter avec les responsables concernés. Une information manquante reste à établir avant la décision qu'elle conditionne.

Champ	Élément à conserver
Périmètre	Activité, système et autorisation concernée
Source	Document ou configuration, date et mode d'observation
Constat	Fait établi et différence avec la situation attendue
Limite	Information manquante ou expertise complémentaire
Action	Responsable, dépendance, coût à instruire et calendrier proposé
Acceptation	Preuve de vérification et décision du responsable

Décision / responsable / échéance :

OUTIL DE TRAVAIL

Répartition des responsabilités

À compléter avec les responsables concernés. Une information manquante reste à établir avant la décision qu'elle conditionne.

Intervenant	Rôle dans la démarche
Direction	Priorités métier, budget et acceptation des étapes
17 SECONDES	Cadrage, audit de préparation, organisation des preuves et AMO
Responsable informatique	Accès, fonctionnement, changements autorisés et maintien
Expert cyber	Évaluations et interventions spécialisées dans son périmètre
Équipes métier	Usages, contraintes et recette des situations réelles
Responsable des données	Conditions de traitement et décisions sur les informations

Décision / responsable / échéance :

POUR APPROFONDIR

Références et prochain échange

Sources publiques consultées le 14 octobre 2026. Les grilles de travail et recommandations de ce document sont proposées par 17 SECONDES.

[1] Cybermalveillance.gouv.fr — Piloter sa cybersécurité. Pilotage par la direction et recours aux spécialistes. [Consulter la source](#)

[2] ANSSI — Guide d'hygiène informatique. Socle de mesures à examiner dans le contexte de l'organisation. [Consulter la source](#)

[3] Cybermalveillance.gouv.fr — Sécuriser son site Internet. Accès, composants, sauvegarde et restauration. [Consulter la source](#)

[4] NIST — Cybersecurity Framework 2.0 for Small Business. Fonctions de gestion du risque cyber. [Consulter la source](#)

[5] CNIL — Déployer une IA générative. Conditions de traitement des données et gouvernance. [Consulter la source](#)

[6] ANSSI — Sécurité d'un système d'IA générative. Sécurisation de l'architecture d'un système d'IA générative. [Consulter la source](#)

Passer de la lecture à une décision

Établir les priorités, organiser une première sécurisation et préparer les projets avec les experts adaptés.

[Prendre rendez-vous avec Gildas Dussauze](#)

contact@17secondes.com · +33 7 56 85 63 29

www.17secondes.com