



**RÉPUBLIQUE
FRANÇAISE**

*Liberté
Égalité
Fraternité*



La directive NIS 2

"Network and Information Security Directive 2" (ou en français : Directive sur la sécurité des réseaux et de l'information 2).

Sommaire

1. Présentation succincte de NIS 2

- a. Entités concernées
- b. La coordination avec d'autres textes
- c. Les objectifs de NIS 2

2. Différence entre NIS 1 et 2

- a. Schéma sur les différences
- b. Remarques

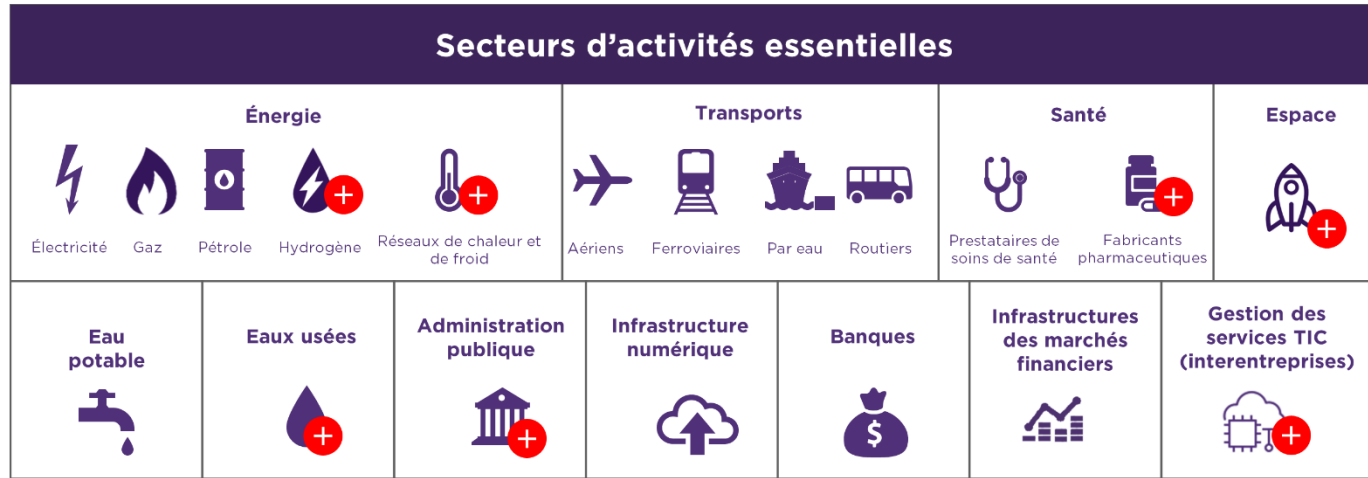
3. Obligations et responsabilités

- a. Mesures de gestion des risques en matière de cybersécurité
- b. Coopération avec l'ANSSI
- c. Sanctions et responsabilités

1-Présentation succincte de NIS 2

- La Directive (UE) 2022/2555, est une directive européenne adoptée le 14 décembre 2022 et entrée en vigueur le 16 janvier 2023. La date limite de la transposition de cette directive était fixée au 17 octobre 2024.
- La France n'a pas encore transposé la directive, le Sénat a adopté la loi de transposition le 11 mars 2025 en première lecture mais pas encore l'Assemblée Nationale.



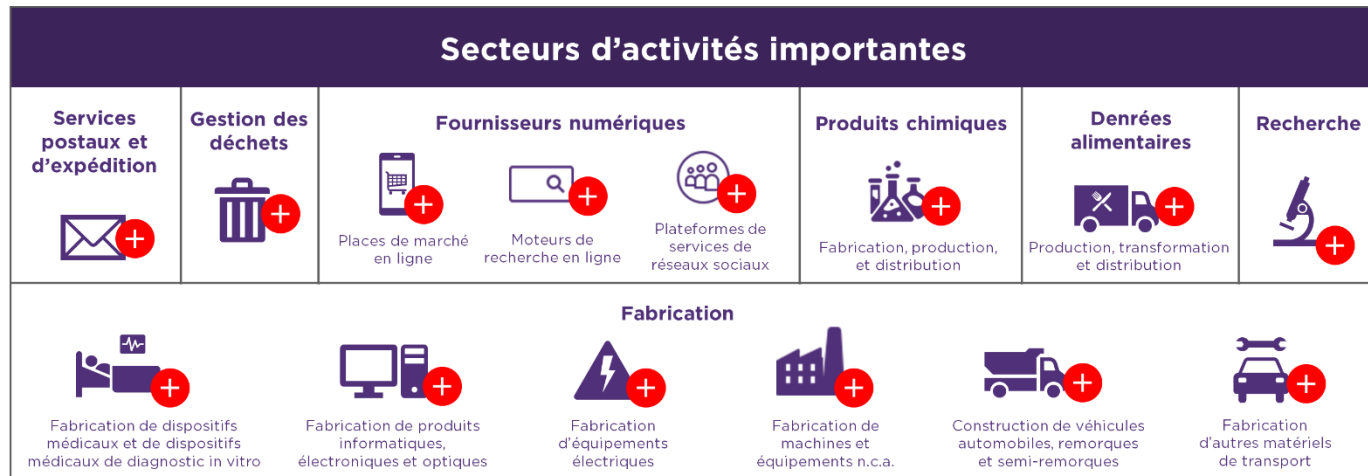


Les entités concernées par la directive NIS 2.

L'ENSFEA sera très probablement concernée par cette directive, le haut fonctionnaire défense et sécurité allait dans ce sens aux dernières nouvelles.

Des consignes du Ministère en charge de l'agriculture sont attendues.

L'objectif est de se préparer à la décision du ministère en anticipant.



+ Secteurs ajoutés par la directive NIS 2

© WAVESTONE

Schéma simplifié pour distinguer Entités Essentielles et Entités Importantes

Taille de l'entité	Nombre d'employés	Chiffre d'Affaires (millions d'euros)	Bilan Annuel (millions d'euros)	Annexe 1	Annexe 2
Intermédiaire et grande	$x \geq 250$	$y \geq 50$	$z \geq 43$	ENTITES ESSENTIELLES	ENTITES IMPORTANTES
Moyenne	$50 \geq x \geq 250$	$10 \geq y > 50$	$10 \geq z > 43$	ENTITES IMPORTANTES	ENTITES IMPORTANTES
Micro et petite	$x < 50$	$y < 10$	$z < 10$	Non concernées	Non concernées

La directive NIS 2 se coordonne avec les textes suivants :

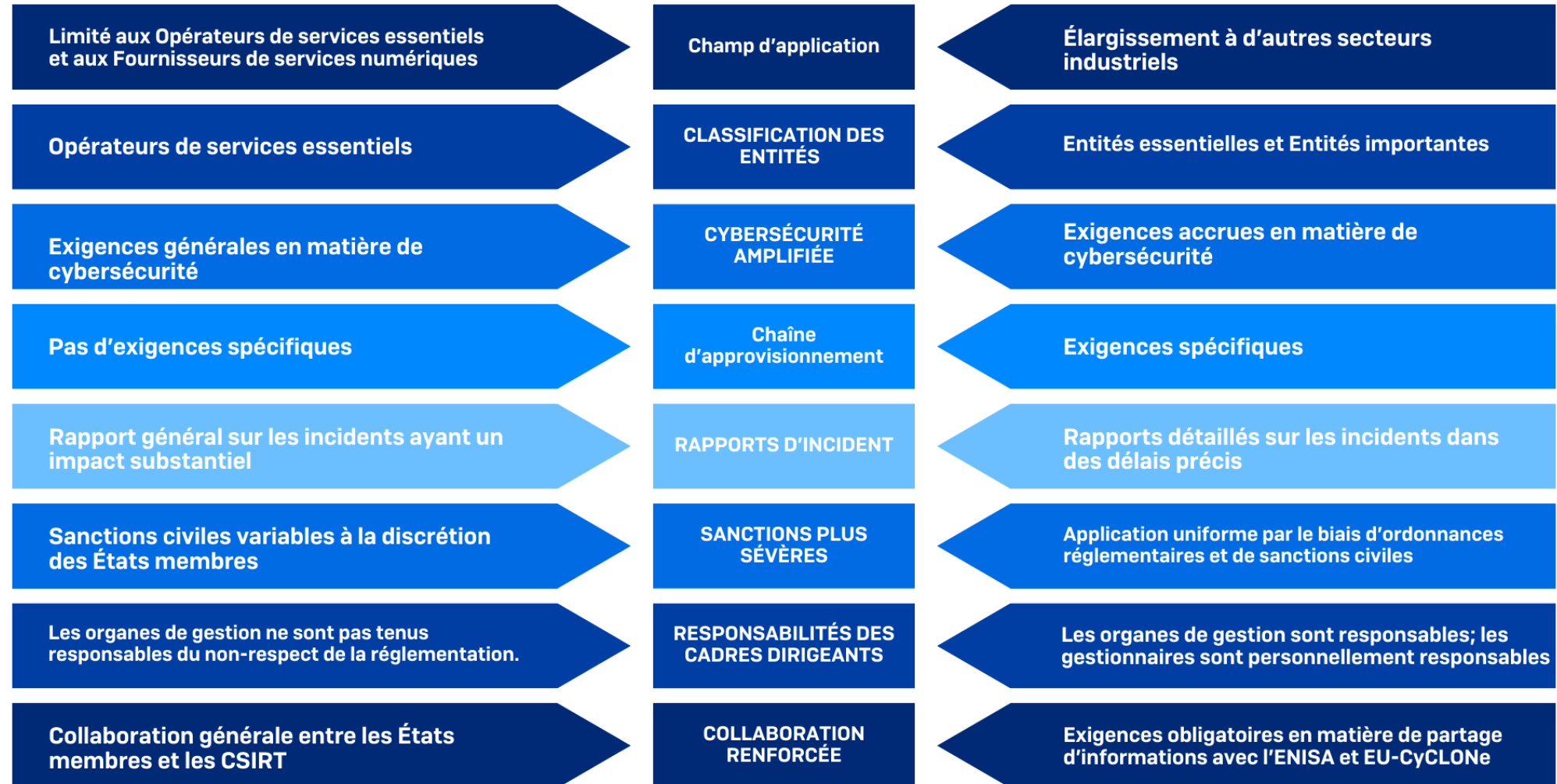
- **La directive relative à la résilience des entités critiques (REC)** : adoptée le 14 décembre 2022, impose aux Etats membres une meilleure préparation aux risques physiques des infrastructures critiques (ex : catastrophes naturelles, sabotage, etc.) ; une coordination accrue à l'échelle de l'UE et des obligations concrètes pour la continuité des services essentiels.
- **Le règlement DORA** : adopté le 14 décembre 2022, traite sur la résilience dans le secteur bancaire et financier.
- **Le règlement cyber-résilience** : adopté le 23 octobre 2024, s'applique à tous les produits contenant des éléments numériques, impose des obligations en matière de cybersécurité sur le software et le hardware du produit.

Les objectifs de NIS 2

- Répondre à l'augmentation phénoménale des cyberattaques dues au contexte géopolitique actuel et à l'amélioration des techniques d'attaques grâce à l'intelligence artificielle.
- Répondre aux nombreuses lacunes de NIS 1 (2016).
- Améliorer la cybersécurité des entités critiques et essentielles au sein de l'UE.
- Renforcer la résilience des réseaux et systèmes d'information.
- Accroître la coopération entre les États membres.
- Harmoniser les obligations de cybersécurité à travers l'Europe

2-Différences entre NIS 1 et NIS 2

Comparaison entre NIS 1 vs NIS 2



Remarques :

- La directive NIS 2 apparaît après la directive NIS 1 considérée comme insuffisante notamment parce que le champ d'application était limité, les obligations pas assez détaillées, pas de délai pour les notifications d'incidents et pouvoir d'enquête et sanctions faibles.
- L'ANSSI estime que près de 15 000 structures seront concernées par NIS 2, contre seulement quelques centaines pour NIS 1.

3-Obligations et responsabilités

Mesures de gestion des risques en matière de cybersécurité (article 21)

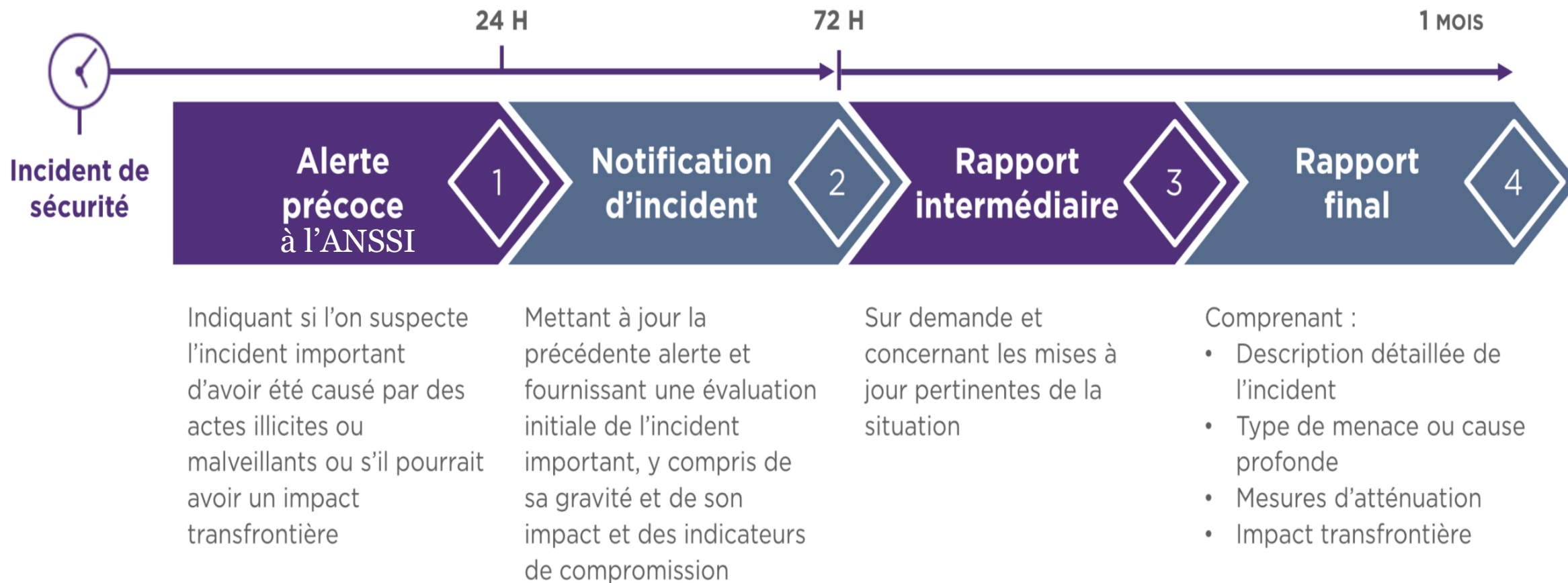
- Les mesures visées au paragraphe 1 sont fondées sur une approche «tous risques» qui vise à protéger les réseaux et les systèmes d'information ainsi que leur environnement physique contre les incidents, et elles comprennent au moins:
 - a) les politiques relatives à l'analyse des risques et à la sécurité des systèmes d'information;
 - b) la gestion des incidents;
 - c) la continuité des activités, par exemple la gestion des sauvegardes et la reprise des activités, et la gestion des crises;
 - d) la sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité concernant les relations entre chaque entité et ses fournisseurs ou prestataires de services directs;
 - e) la sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information, y compris
- le traitement et la divulgation des vulnérabilités;

- f) des politiques et des procédures pour évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité;
- g) les pratiques de base en matière de cyber hygiène et la formation à la cybersécurité;
- h) des politiques et des procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement;
- i) la sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs;
- j) l'utilisation de solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence au sein de l'entité, selon les besoins.

Coopération avec l'ANSSI

- Le rôle de l'ANSSI est renforcé :
- elle accompagnera les structures pour la mise en conformité, les pouvoirs de contrôle sont augmentés et les sanctions sont plus sévères.
- Les entités soumises à NIS 2 doivent se déclarer auprès de l'ANSSI, c'est leur responsabilité.
- Elles doivent identifier les systèmes d'informations critiques et spécifier les services essentiels qui en dépendent. (ex : fourniture d'accès à internet)
- Elles doivent réaliser des analyses de risques, identifier les menaces, mettre en place des mesures techniques et organisationnelles. Il faut un plan de résilience global.
- Elles doivent obligatoirement notifier les incidents à l'ANSSI (en plus de la CNIL si cela concerne des données personnelles) sous peine de sanctions.

La procédure à appliquer à la découverte d'un incident de sécurité



Notifier à l'ANSSI (site de l'ANSSI, contacter)

Publié le 22 Juillet 2022 • Mis à jour le 13 Juin 2025

En cas d'incident ou de découverte de vulnérabilité chez vous ou chez autrui, veuillez vous référer à [cette page](#).

Si vous êtes victime de cybermalveillance, veuillez consulter [cette page](#).

Si vous souhaitez contacter les délégués de l'ANSSI dans les territoires, veuillez consulter [cette page](#).

Contacteur l'ANSSI par courrier électronique :

- Pour signaler un incident, une menace de sécurité informatique ou une vulnérabilité chez vous ou chez autrui : **cert-fr [at] ssi.gouv.fr**
- Pour faire connaître votre solution/votre entreprise à l'Agence ; faire évaluer une solution et valoriser votre Visa de sécurité ANSSI ; demander une clarification sur un référentiel d'exigences, de la réglementation ou de la normalisation ; recevoir la newsletter « ANSSI Industrie » dédiée aux offreurs : **industries [at] ssi.gouv.fr**
- Pour déposer une demande de d'agrément ou de qualification d'un produit ou d'un service, ou pour déclarer un incident de sécurité ou une vulnérabilité affectant ou susceptible d'affecter un service ou un produit agréé ou qualifié : **qualification [at] ssi.gouv.fr**
- Pour déposer un dossier d'enregistrement ou déclarer une vulnérabilité sur un produit certifié : **certification [at] ssi.gouv.fr**
- Pour les démarches réglementaires relatives aux produits de cryptologie (procédures prévues notamment par le décret n°2007-663 et le règlement UE 2021/821), aux appareils et dispositifs techniques de nature à permettre l'atteinte à la sécurité des correspondances (procédure prévue par les articles R226-1 et suivants du code pénal) et à certains équipements de réseau de communications électroniques mobiles de cinquième génération (procédure prévue par l'article L.34-11 du code des postes et des communications électroniques) : **controle [at] ssi.gouv.fr**
- Pour contacter le Centre national de coordination cyber français (NCC-FR) et être accompagné dans la réponse à un appel à projet européen : **ncc-fr.anssi [at] ssi.gouv.fr**
- Pour toute question simple portant sur les guides techniques de l'Agence en particulier : **conseil.technique [at] ssi.gouv.fr**
- Pour toute demande concernant le recrutement à l'ANSSI : **recrutement [at] ssi.gouv.fr**
- Pour toute demande concernant les formations proposées par l'Agence ou SecNumAcadémie, le MOOC de l'ANSSI : **cfssi [at] ssi.gouv.fr**
- Pour toute demande presse (interviews, tournages, etc.) : **presse [at] ssi.gouv.fr**
- Pour toute demande relative aux événements (intervention d'un agent de l'ANSSI dans la programmation ou demande d'exposition sur un salon) : **evenements [at] ssi.gouv.fr**

Accueil > Accueil espace 17Cyber > Diagnostic



Diagnostic 17Cyber

Vous pensez être victime d'un acte de cybermalveillance ? Notre dispositif conseille et oriente les victimes de cybermalveillance. L'outil de diagnostic en ligne va vous permettre d'identifier votre problème et vous proposer des conseils personnalisés pour pouvoir y faire face.

Les grandes étapes de la démarche

⌚ 10 minutes pour effectuer la démarche

1 Questionnaire

Laissez-vous guider pour détailler le problème que vous rencontrez, en répondant à nos questions pas à pas.

- Votre profil
- Votre problème

2 Récapitulatif

Relisez les réponses que vous avez renseignées avant de les confirmer, ou modifiez-les si nécessaire.

3 Résultats

Le résultat de ce questionnaire nous permettra d'établir un diagnostic personnalisé par rapport à la situation dont vous êtes victime, et de vous proposer les solutions adaptées.

Je commence le questionnaire

Avant de commencer la démarche

Aucune information à caractère personnel ne vous sera demandée pour obtenir votre diagnostic.

Gouvernance (art.20)

- Les dirigeants doivent suivre une formation en cybersécurité. Les entités sont également encouragées à former régulièrement leurs équipes, afin de renforcer la capacité à gérer les risques cyber.
- Les organes de direction doivent approuver et superviser les mesures de cybersécurité mises en place. Ils peuvent être tenus responsables en cas de non-respect des obligations légales (article 21).
- Réaliser un audit de sécurité pour évaluer leur niveau de maturité
- Définir une stratégie de cybersécurité adaptée à leurs besoins
- Mettre en place une organisation et une gouvernance efficace
- Sensibiliser et former leur personnel

Sanctions en cas de non-conformité (art.34)

« 4. Les États membres veillent à ce que, lorsqu'elles violent l'article 21 ou 23, les entités essentielles soient soumises, conformément aux paragraphes 2 et 3 du présent article, à des amendes administratives d'un montant maximal s'élevant à **au moins 10 000 000 EUR ou à au moins 2 % du chiffre d'affaires annuel mondial total** de l'exercice précédent de l'entreprise à laquelle l'entité essentielle appartient, le montant le plus élevé étant retenu.

5. Les États membres veillent à ce que, lorsqu'elles violent l'article 21 ou 23, les entités importantes soient soumises, conformément aux paragraphes 2 et 3 du présent article, à des amendes administratives d'un montant maximal s'élevant **à au moins 7 000 000 EUR ou à au moins 1,4 % du chiffre d'affaires annuel mondial total** de l'exercice précédent de l'entreprise à laquelle l'entité importante appartient, le montant le plus élevé étant retenu. »

Merci pour votre attention

- Sources :
- *Directive NIS 2*
- *Wavestone*
- *Sophos*
- *ANSSI*