AMRAE

la Maison du risk management

COMMISSION CYBER

PRÉSIDÉE PAR PHILIPPE COTELLE

QUELS CHANGEMENTS AVEC LA DIRECTIVE NIS 2 ?

Mathieu COUTURIER, ANSSI

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

AMRAE

QUELS CHANGEMENTS AVEC LA DIRECTIVE NIS 2 ?

AMRAE – COMMISSION CYBER

18 AVRIL 2024

Mathieu COUTURIER – Chef de division adjoint – Management de la sécurité numérique
mathieu.couturier@ssi.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

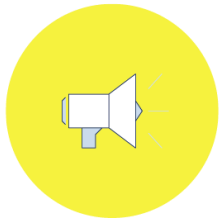
1. PRÉSENTATION DE L'ANSSI

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

L'ANSSI

Agence nationale de la sécurité des systèmes d'information créée en 2009 – 650 agents

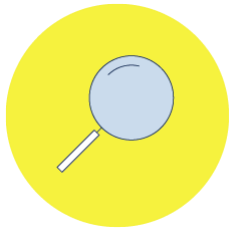
Mission défensive (et non offensive)



Autorité nationale en matière de cybersécurité et de cyberdéfense

Rôle : protéger la Nation face aux cyberattaques

Service du Premier ministre rattaché au Secrétariat général de la défense et de la sécurité nationale (SGDSN)



Cibles premières : OIV (opérateurs d'importance vitale), OSE (opérateurs de services essentiels) et administrations

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

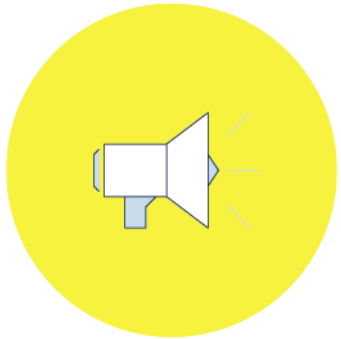
Les principales missions de l'ANSSI

Défendre

les systèmes d'information critiques et les victimes de cyberattaques d'ampleur

Connaître

l'état de l'art de la cybersécurité et les menaces du cyberespace



Partager

de la connaissance, des recommandations et de l'expertise en sécurité numérique

Accompagner

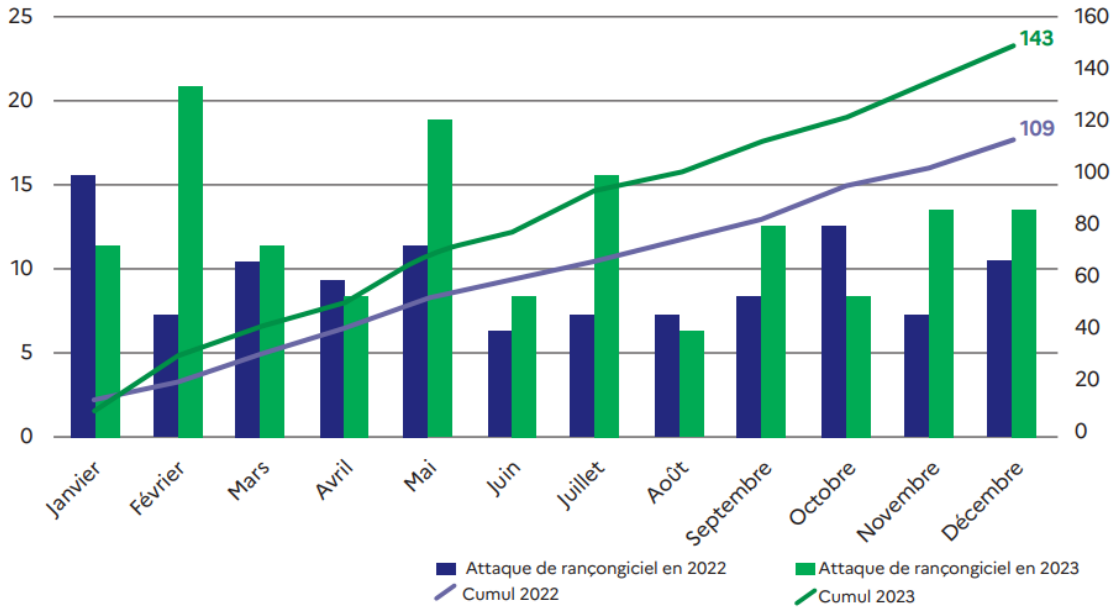
l'écosystème national et international

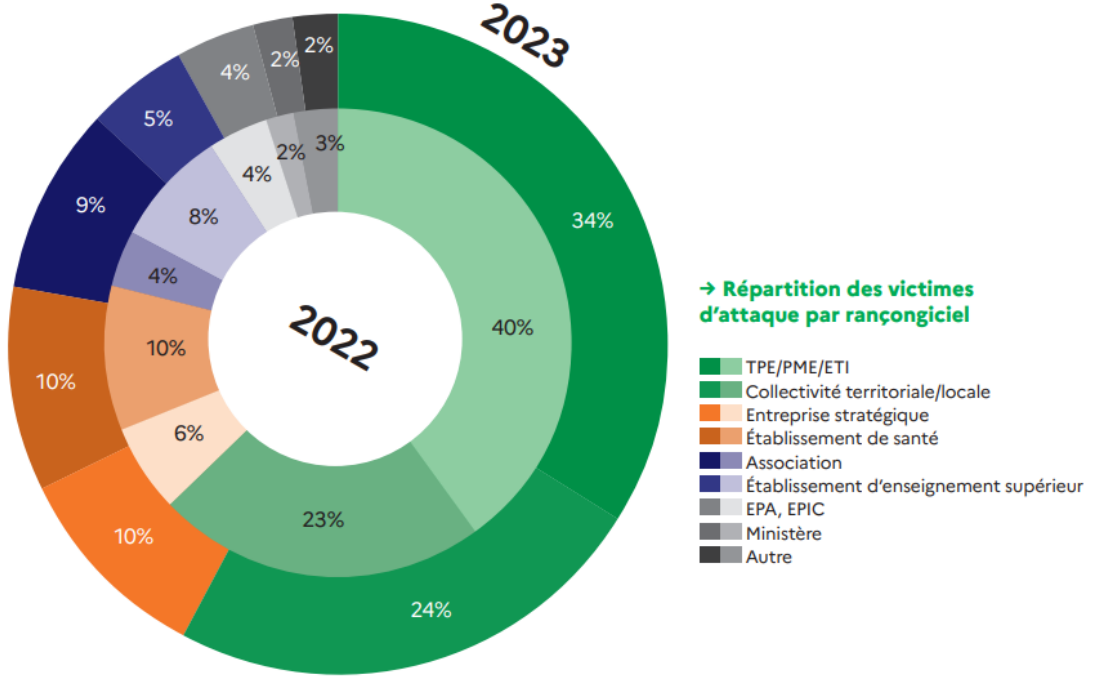
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

UNE MENACE CYBER DE PLUS EN PLUS PRÉGNANTE ET IMPACTANTE

Une évolution nécessaire à l'échelle européenne

→ Comparaison des signalements d'attaques par rançongiciel en 2022 et 2023





Source : ANSSI - panorama de la menace 2023

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

NIS2 : LA RÉPONSE À L'ÉVOLUTION DE LA MENACE CYBER

La directive en synthèse

Elever le niveau de cyber sécurité du marché intérieur de l'UE : cybersécurité des opérateurs critiques (NIS1) vers la cybersécurité de masse (NIS2)

LUTTER CONTRE LA CYBERCRIMINALITÉ DE MASSE

- Se protéger des rançongiciels
- Sensibiliser
- Former des dirigeants

18 SECTEURS CONCERNÉS

- 17 secteurs d'activité
  - Entreprises de plus de 50 employés ou plus de 10M€ de CA ou bilan
- Administration
  - administration centrale
  - collectivités locales

TRANSPOSITION NATIONALE

- Obligation incombant aux Etats Membres (Oct. 2024)
- Production des textes législatifs et réglementaires
- Acteurs du numérique : AE rédigé par la commission européenne (Oct. 2024)

TLP:AMBER

NIS2 : les obligations pour les entités régulées

NIS 2 intègre deux typologies d'entités différentes :
Les entités essentielles (**EE**)
Les entités importantes (**EI**)
➔ suppression du mécanisme unique de désignation et intégration de seuils

Des obligations communes : **Notification, contact et déclaration des incidents majeurs**

- **Notification à l'ANSSI** - mécanisme mis en place pour se notifier auprès de l'ANSSI
- **Communication des informations de contact** et mise à jour (yc. liste des Etats membres de l'UE dans lesquels sont fournis les services)
- **Déclaration à l'ANSSI des incidents majeurs** (notification > rapport d'avancement > rapport final)

Au regard de NIS 1

- Suppression de la notion de service essentiel
- Extension du périmètre des systèmes d'information à sécuriser qui n'est plus restreint aux « systèmes d'information essentiels »

TLP:AMBER

NIS2 : les obligations pour les entités régulées

NIS 2 intègre deux typologies d'entités différentes :
Les entités essentielles (**EE**)
Les entités importantes (**EI**)
➔ suppression du mécanisme unique de désignation et intégration de seuils

NIS 2 intègre la proportionnalité entre **EE** et **EI** dans :

Les mesures de sécurité
- Possibilité d'avoir des niveaux d'exigences différents entre les **EE** et les **EI**, notamment pour prendre en considération les moyens et enjeux d'une grande entreprise versus d'une PME.

La régulation
- Pour les **EE** : régulation dite « ex-ante » (contrôle à discrétion de l'ANSSI)
- Pour les **EI** : régulation dite « ex-post » (contrôle en cas de connaissance d'une non-conformité)

Les sanctions
- Seront d'une ampleur comparable à celui du RGPD
- De manière simplifiée, sanctions pouvant aller jusqu'à 2% du CA mondial pour les **EE** et 1,4% pour les **EI**

Au regard de NIS 1
- Suppression de la notion de service essentiel
- Extension du périmètre des systèmes d'information à sécuriser qui n'est plus restreint aux « systèmes d'information essentiels »

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

TLP:AMBER

NIS2 : périmètres pour les EE et les EI

SCHÉMATISATION SIMPLIFIÉE DE LA RÈGLE DE BASE

TAILLE ENTITE	NOMBRE D'EMPLOYÉS	CHIFFRE D'AFFAIRES (MILLIONS D'EUROS)	BILAN ANNUEL (MILLIONS D'EUROS)	ANNEXE 1	ANNEXE 2
INTERMÉDIAIRE ET GRANDE	Supérieur à 250	Supérieur à 50	Supérieur à 43	ENTITES ESSENTIELLES	ENTITES IMPORTANTES
MOYENNE	Entre 50 et 250	Entre 10 et 50	Entre 10 et 43	ENTITES IMPORTANTES	ENTITES IMPORTANTES

A noter des seuils spécifiques pour les acteurs du numérique

TLP:AMBER

Focus sur les secteurs d'activité concernés par la directive

Annexe1:

SECTEUR	SOUS-SECTEUR
01. ÉNERGIE	Électricité
	Réseaux de chaleur et de froid
	Pétrole
	Gaz
	Hydrogène
02. TRANSPORTS	Transports aériens
	Transports ferroviaires
	Transports par eau
	Transports routiers
03. SECTEUR BANCAIRE	
04. INFRASTRUCTURES DES MARCHÉS FINANCIERS	
05. SANTÉ	
06. EAU POTABLE	
07. EAUX USÉES	
08. INFRASTRUCTURE NUMÉRIQUE	
09. GESTION DES SERVICES TIC	
10. ADMINISTRATION PUBLIQUE	Administration centrale
11. ESPACE	

Annexe 2:

SECTEUR	SOUS-SECTEUR
01. SERVICES POSTAUX ET D'EXPÉDITION	
02. GESTION DES DÉCHETS	
03. FABRICATION, PRODUCTION ET DISTRIBUTION DE PRODUITS CHIMIQUES	
04. PRODUCTION, TRANSFORMATION ET DISTRIBUTION DES DENRÉES ALIMENTAIRES	
05. FABRICATION	Fabrication de dispositifs médicaux et de dispositifs médicaux de diagnostic in vitro
	Fabrication de produits informatiques, électroniques et optiques
	Fabrication d'équipements électriques
	Fabrication de machines et équipements
	Construction de véhicules automobiles, remorques et semi-remorques
	Fabrication d'autres matériels de transport
06. FOURNISSEURS NUMÉRIQUES	
07. RECHERCHE	

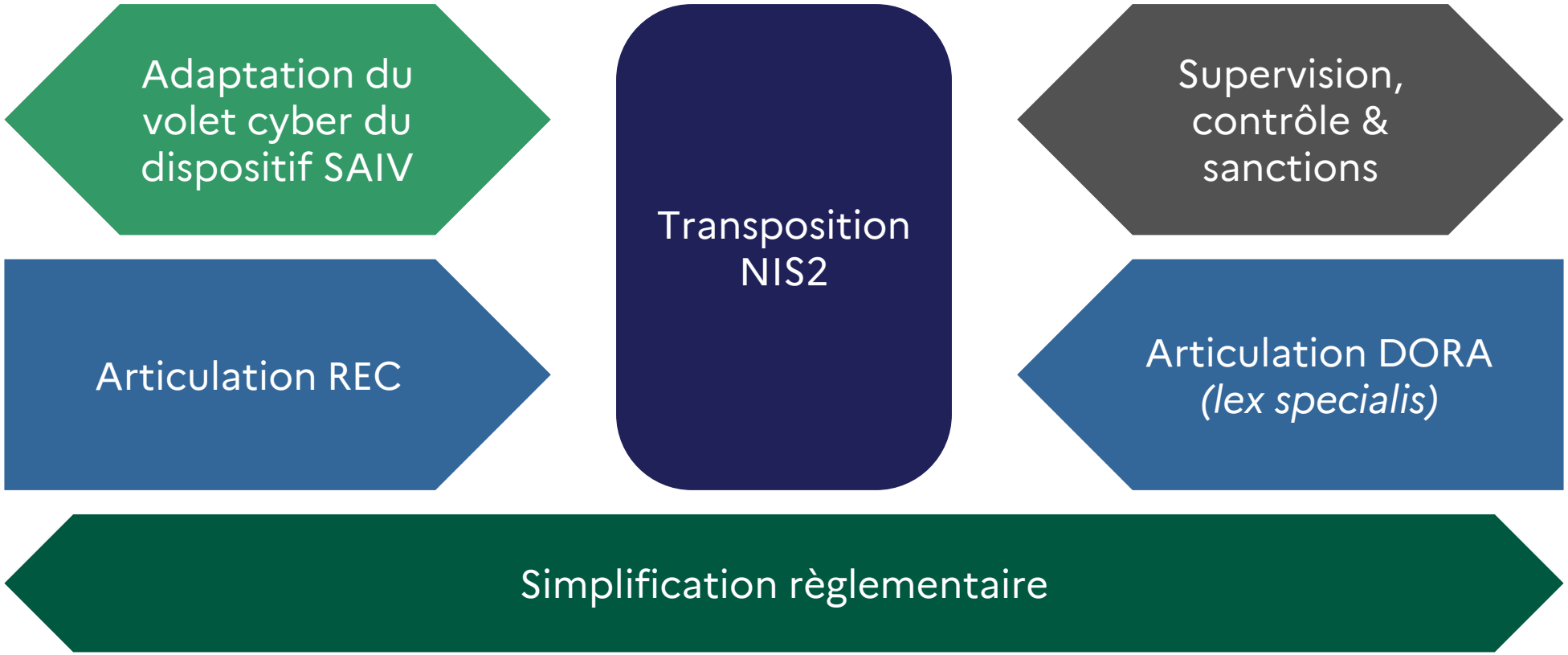
- La France aura la possibilité **d'intégrer unitairement**, et à la marge, des entités ne respectant pas les critères de base sur la base d'une analyse de risque nationale.

- La France aura également la possibilité **d'exclure unitairement** des entités au regard de la clause de défense et de sécurité nationale prévue par la directive.

FOCUS SUR LA TRANSPOSITION NATIONALE DE LA DIRECTIVE

Transposition de la directive : le projet de loi cyber

Un principe structurant : absence de surtransposition



TLP:AMBER

Transposition de la directive NIS 2 pour les mesures de gestion des risques

Un principe structurant : intégration forte de la proportionnalité

TLP:AMBER

Focus sur le champ des règles

Entités Essentielles
Centres de gravité

Entités Importantes
Masse critique

Analyse de risques
Homologation (gouvernance de la sécurité)
Gestion des tiers (*supply-chain*)
Périmètre des SI
Ajout d'exigences sur les annuaires
Gestion de crise & entrainement

Approche par conformité sur la base d'une analyse faite par l'ANSSI
Hygiène de base
Acceptabilité du BYOD
Continuité d'activité centrée autour de la sauvegarde

Pas d'obligation de recourir à des prestataires ou des solutions qualifiés par l'ANSSI
➔ recommandation d'y faire appel

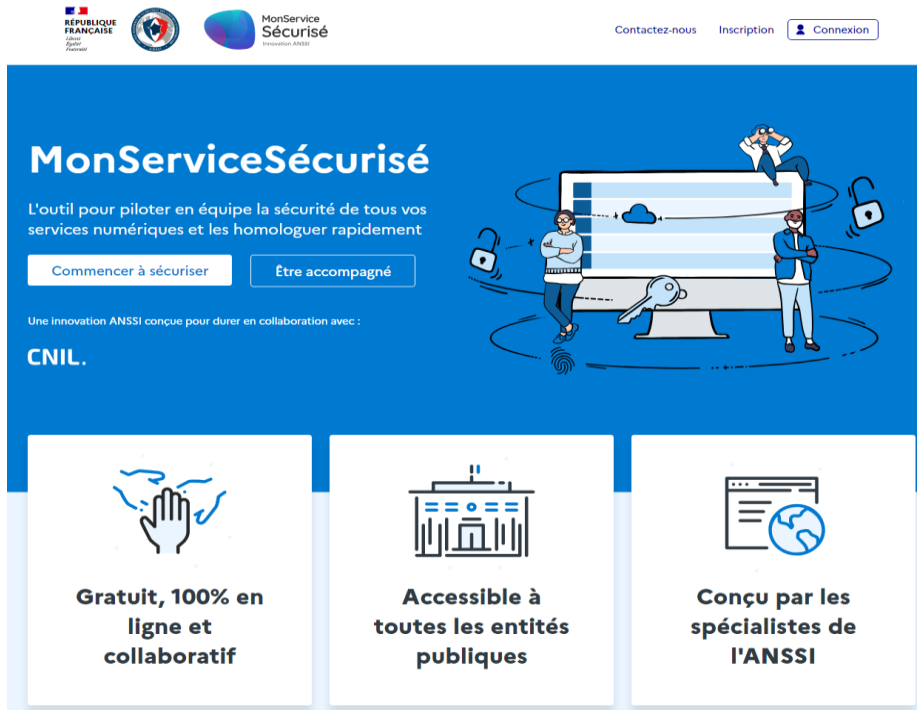
TLP:AMBER

Accompagnement

Un dispositif de services numériques pour démultiplier l'accompagnement de l'Agence

https://monespacenis2.cyber.gouv.fr/

https://monservicesecurise.ssi.gouv.fr/



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

NIS2…LE SEUL TEXTE EUROPÉEN ?

Cyber Résilience Act (CRA), l'autre texte européen d'ampleur

➔ Règlement européen (sans transposition nationale), accord politique en décembre 2023 (application 2024)

➔ Imposera des exigences de sécurité basiques à tous les produits numériques vendus sur le marché européen (produits comportant des éléments numériques), en termes de caractéristiques des produits, mais aussi de processus.

➔ Focus important sur la gestion des vulnérabilités et la notification à l'autorité nationale

➔ Fabricants, importateurs et distributeurs de matériels et de logiciels auront 36 mois après publication du texte pour appliquer le texte et 21 mois pour la notification des incidents

Partage des responsabilités entre les fournisseurs du numérique soumis au CRA et les utilisateurs du numérique régulés par NIS2.

Liste des ressources à disposition

➔ MonAideCyber (ssi.gouv.fr)

➔ **Webinaire de présentation de la directive : Webinaire NIS 2 : présentation de la directive et de sa transposition nationale | ANSSI (cyber.gouv.fr)**

➔ **Page dédiée et FAQ sur la directive : La directive NIS 2 | ANSSI (cyber.gouv.fr)**

➔ **Les guides essentiels :**

- ➔ Panorama de la menace 2023 Le Panorama de la cybermenace | ANSSI
- ➔ Gestion et communication des crises d'origine cyber : Anticiper et gérer une crise Cyber | ANSSI
- ➔ Kit d'exercice de crise prêt à l'emploi : Organiser un exercice de gestion de crise cyber | ANSSI
- ➔ 42 mesures d'hygiène informatique : Guide d'hygiène informatique | ANSSI (cyber.gouv.fr)
- ➔ Méthodologie d'analyse de risques « Ebios Risk Manager » (nouvelle version) : La méthode EBIOS Risk Manager - Le guide | ANSSI (cyber.gouv.fr)

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

QUESTIONS