RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CRE COMMISSION DE RÉGULATION DE L'ÉNERGIE

Groupe de travail cybersécurité de la CRE avec le soutien de l'ANSSI

3 avril 2026

Agenda

		Mot d'accueil
14h00 – 14h10	**0h10**	**Flash info sur les travaux européens** - Code réseau cybersécurité
14h10 – 14h30	**0h20**	**Panorama de la Cybermenace 2025**
14h30 – 14h50	**0h20**	**Ciblage de la production d'Énergie électrique et du secteur de l'eau en France** - Constats et recommandations
14h50 – 15h15	**0h25**	**NIS2 & publication du Référentiel Cyber France** - ReCyF
15h15 – 15h25	**0h05**	**Actus Cyber**
		Clôture

01.

Flash info sur les travaux européens

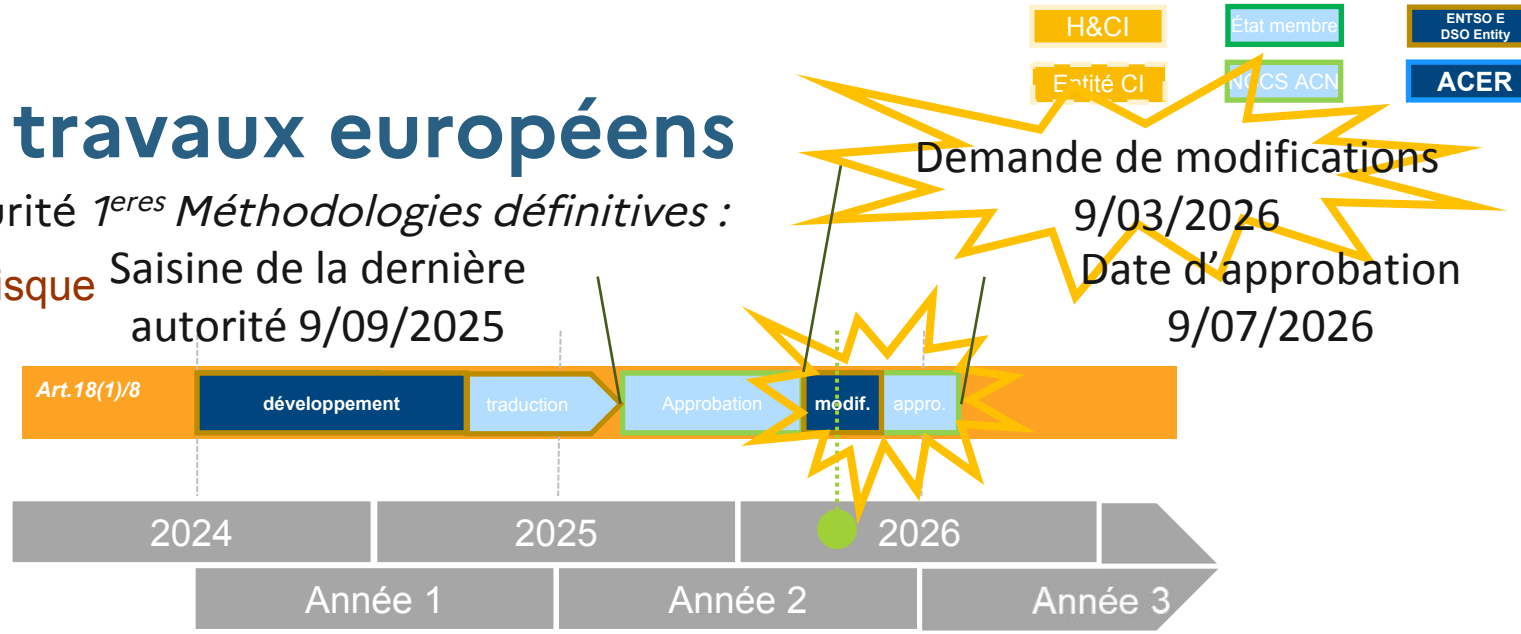
Sujets

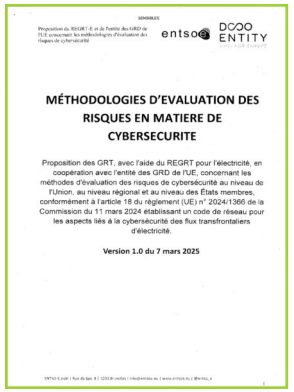
- Code réseau cybersécurité

Retour sur les travaux européens

Code de réseau cybersécurité *1eres Méthodologies définitives :*

Méthodologie d'analyse de risque





MÉTHODOLOGIES D'EVALUATION DES RISQUES EN MATIERE DE CYBERSECURITE

Proposition des GRT, avec l'aide du REGRT pour l'électricité, en coopération avec l'entité des GRD de l'UE, concernant les méthodes d'évaluation des risques de cybersécurité au niveau de l'Union, au niveau régional et au niveau des États membres, conformément à l'article 18 du règlement (UE) n° 2024/1366 de la Commission du 11 mars 2024 établissant un code de réseau pour les aspects liés à la cybersécurité des flux transfrontaliers d'électricité.

Version 1.0 du 7 mars 2025

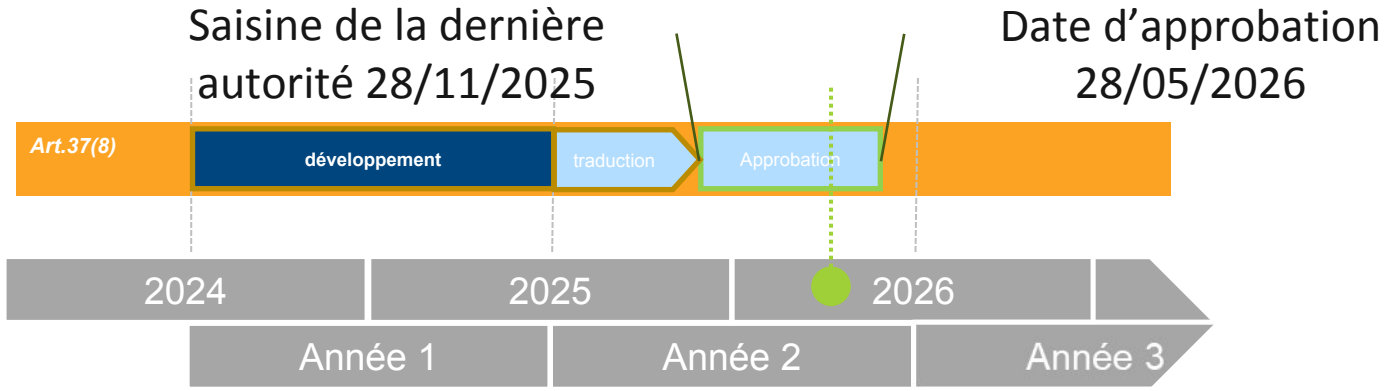
- La méthodologie permettra d'établir les ECII, permettant de désigner les entités I F&C.
  Elle permettra aussi d'établir les processus I F&C qui seront utilisés dans les évaluations des risques au niveau de l'entité et des États membres.
  Elle permettra d'élaborer de mesures de cybersécurité minimales et avancées.

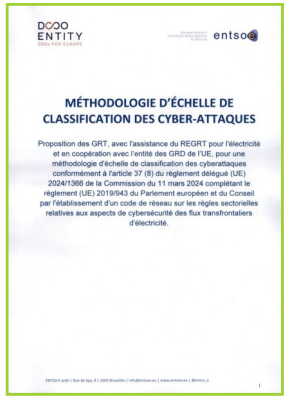
H&CI | État membre | ENTSO E DSO Entity | Niveau européen
Entité CI | NCCS ACN | ACER | Niveau National | Niveau Entité

Retour sur les travaux européens

Code de réseau cybersécurité *1eres Méthodologies définitives :*

Méthodologie de classement des cyberattaques




DSOO ENTITY
entsoe
MÉTHODOLOGIE D'ÉCHELLE DE CLASSIFICATION DES CYBER-ATTAQUES
Proposition des GRT, avec l'assistance du REGRT pour l'électricité et en coopération avec l'entité des GRD de l'UE, pour une méthodologie d'échelle de classification des cyberattaques conformément à l'article 37 (8) du règlement délégué (UE) 2024/1366 de la Commission du 11 mars 2024 complétant le règlement (UE) 2019/943 du Parlement européen et du Conseil par l'établissement d'un code de réseau sur les règles sectorielles relatives aux aspects de cybersécurité des flux transfrontaliers d'électricité.

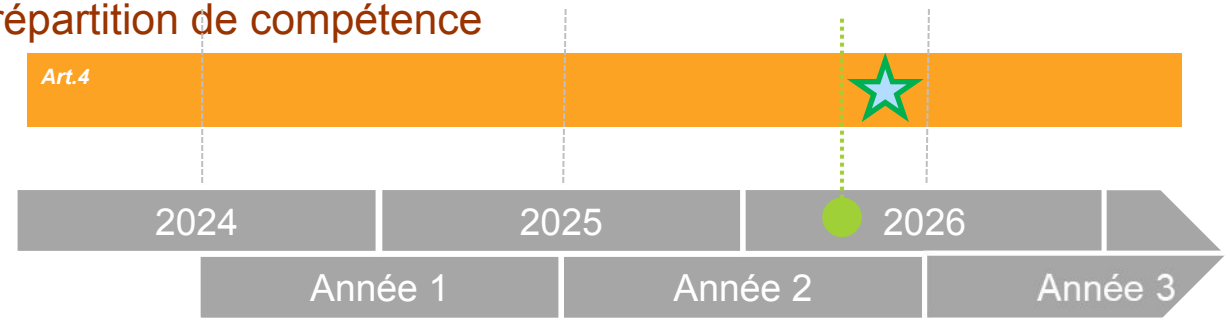
- L'impact potentiel déterminé par les actifs touchés
  La gravité de l'attaque est déterminée par la profondeur de l'attaque

H&CI | État membre | ENTSO E DSO Entity | Niveau européen
Entité CI | NCCS ACN | ACER | Niveau National | Niveau Entité

Retour sur les travaux européens

Code de réseau cybersécurité *désignation de l'autorité compétente :*

Décret de nomination et de répartition de compétence



Projet

- Désignation du ministère en charge de l'énergie en tant qu'autorité compétente (tâches métier)
- Possibilité de délégation à l'ANSSI (tâches cyber)
- Pas de délégation à la CRE (qui conserve ses prérogatives tarifaires couverture des coûts des gestionnaires art. 11 et benchmark art. 13)

ÉCHÉANCES ORGANISATIONNELLES ET TRANSITOIRES

ÉM | ARN | GRT | ACER | ARNs

Niveau européen | Niveau national

Désignation de l'autorité compétente –*Art.4*

Orientations optionnelles sur les informations pertinentes pour la mise en œuvre du code –*Art 12(3)*

Rapport de mise en œuvre | Rapport de mise en œuvre | Rapport de mise en œuvre –*Art 12(1)*

Guide non contraignant d'évaluation comparative en matière de cybersécurité –*Art 13 (1)*

Évaluation comparative –*Art 13 (2)*

Analyses de coûts des GRD et GRT et couverture par les tarifs d'utilisation des réseaux –*Art 11*

Accords avec des GRT extérieurs à l'Union –*Art 14*

Lignes directrices concernant les échanges des informations –*Art 47 (7)*

Art.48(2) Seuils transitoires

Art.48(3) Liste E IF&C transitoire

Art.48(3) Notification E IF&C transitoires | Analyse de risques volontaires des E IF&C transitoires

Art.48(4) Processus IF&C

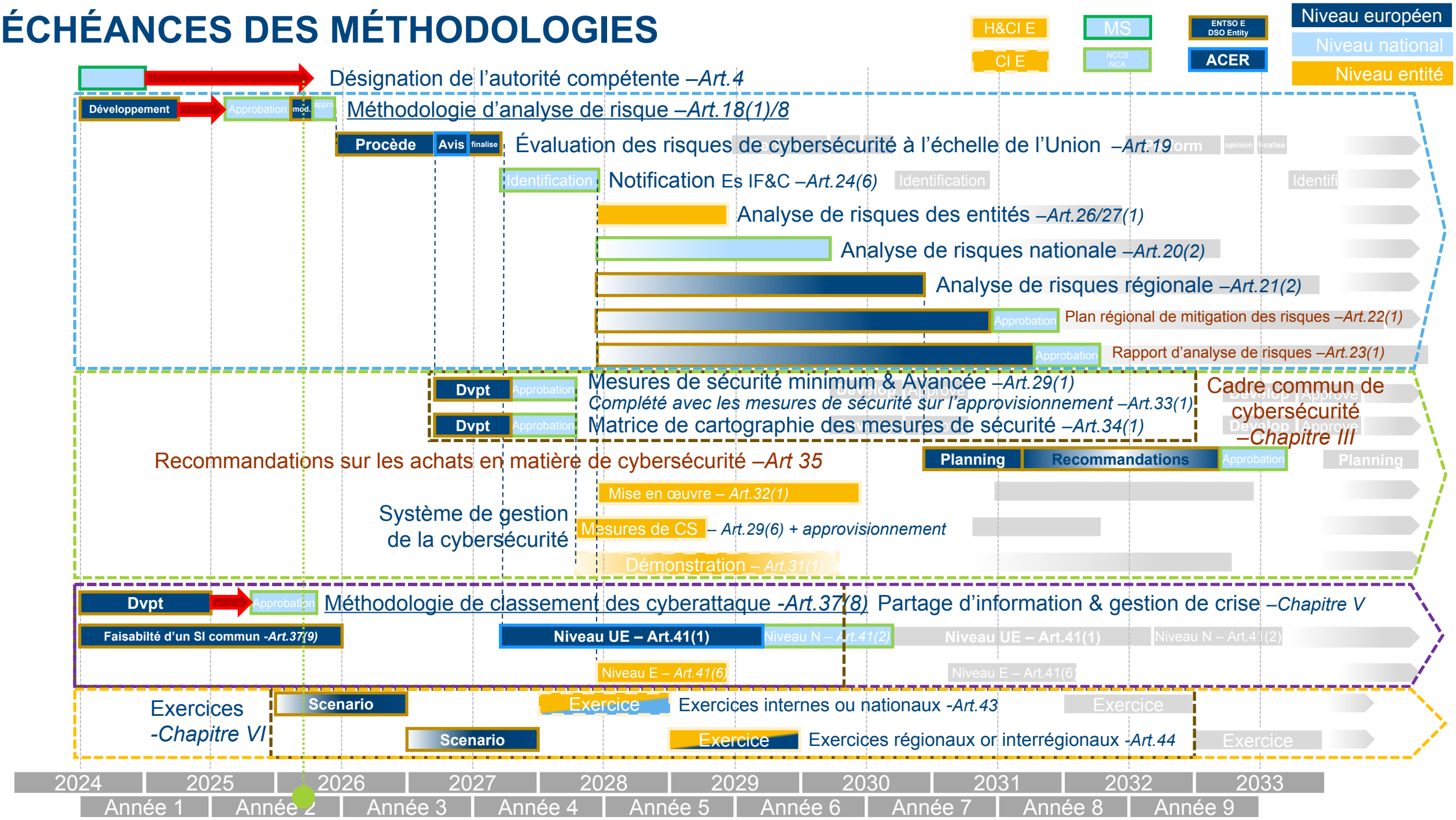
Art.48(5) Liste leg. nationales

Art.48(6) Liste transitoire des normes et des mesures de sécurité

Mesures transitoires –*Art 48*

2024	2025	2026	2027	2028	2029	2030	2031	2032	2033
Année 1	Année 2	Année 3	Année 4	Année 5	Année 6	Année 7	Année 8	Année 9	

ÉCHÉANCES DES MÉTHODOLOGIES



02.

Panorama de la Cybermenace 2025

Introduction et contexte général

La menace reste élevée et de plus en plus hybride

Contexte mondial de la cybermenace

- 2025 marqué par une menace persistante et systémique

Attaque destructrice en Pologne

- Première attaque coordonnée contre infrastructures électriques d'un État membre de l'UE
- Objectif : provoquer des coupures d'électricité et de chauffage

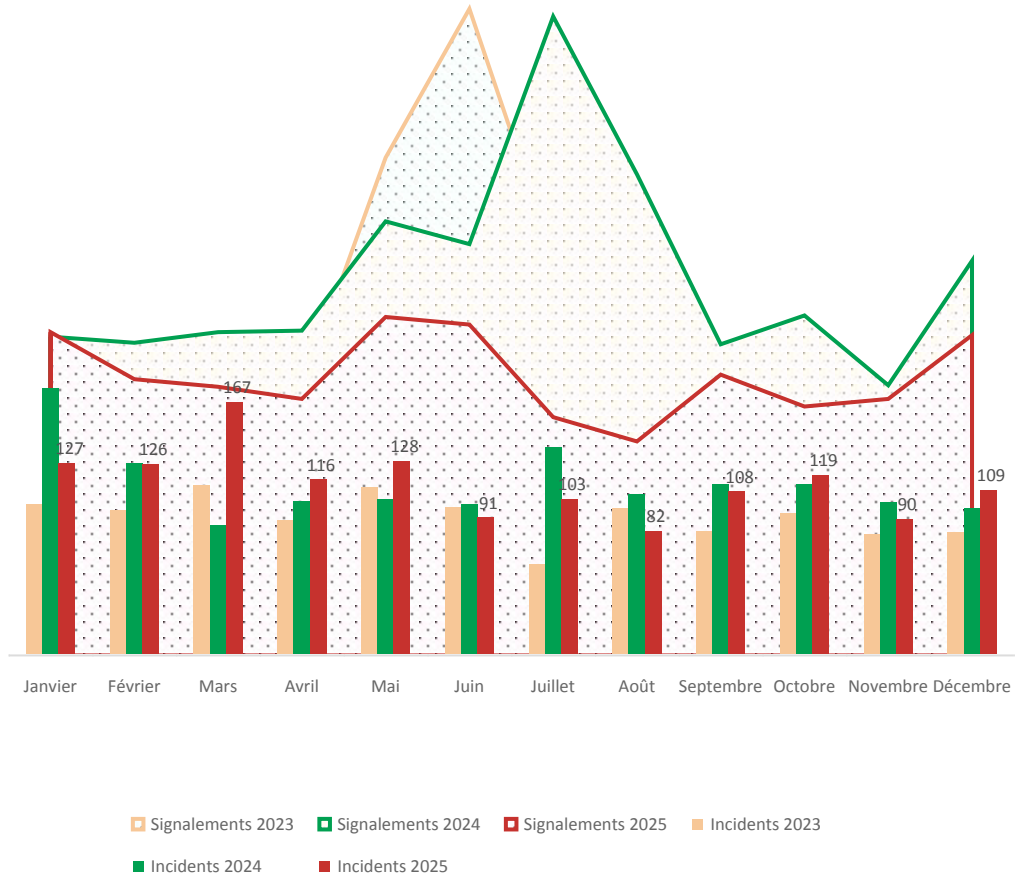
Préparation et anticipation en France

- France se prépare à une hausse massive des attaques hybrides d'ici 2030
- Accent sur la résilience des infrastructures critiques

L'incidentologie en 2025

Une vue comparative sur les 3 dernières années

- Au cours de l'année 2025, l'ANSSI a traité, avec un degré d'engagement variable, 3586 événements de sécurité, soit une diminution de 18% par rapport à l'année 2024



Extorsion de fond

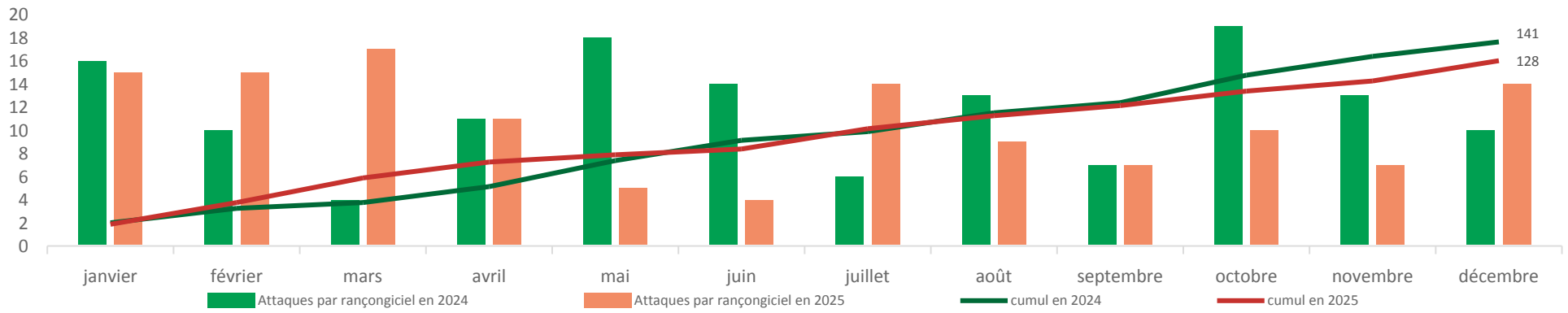
Par des acteurs cybercriminels

Les rançongiciels

- Une menace qui touche l'ensemble des secteurs et des zones géographiques
- En France, légère baisse d'activité en 2025 observée par l'ANSSI
- Les PME/TPE/ETI restent la catégorie d'entités la plus affectée, suivi des collectivités territoriales et des établissements de santé
- Les établissements scolaires ont été particulièrement touchés en 2025

Les exfiltrations de données

- 196 incidents relatifs à des exfiltrations de données associées ou non à des attaques par rançongiciels (130 en 2024)
- Fait notable : certaines revendications reprennent des données publiques ou précédemment divulguées

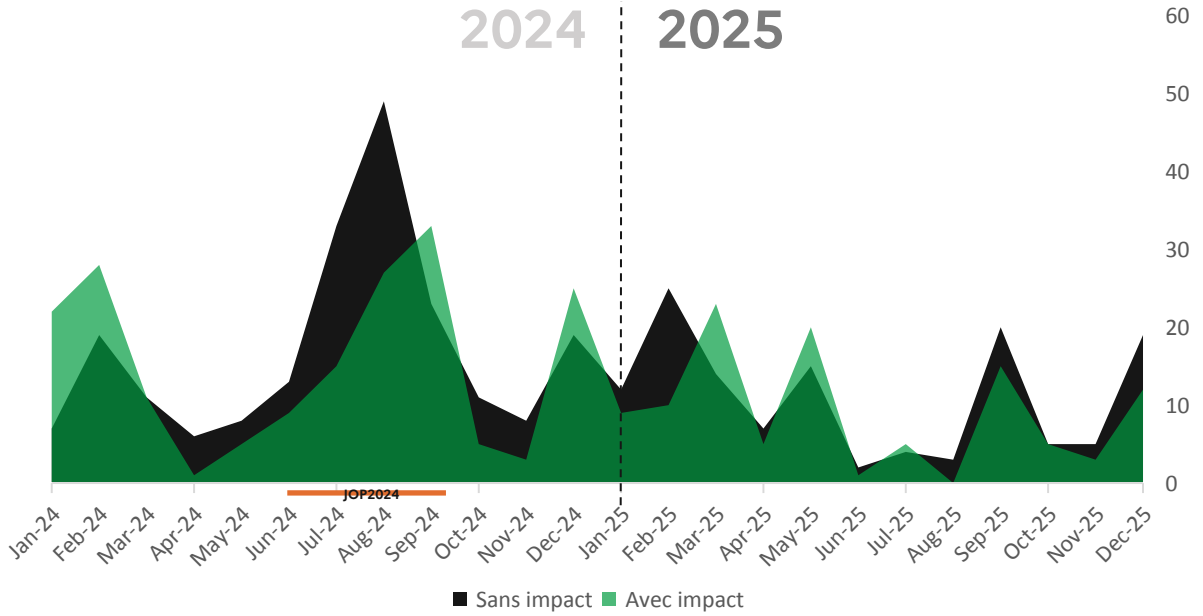


Attaques par déni de service distribué (DDoS)

Maintien d'un bruit de fond continu par des acteurs malveillants

ATTAQUES PAR DÉNI DE SERVICE DISTRIBUÉ (DDOS)

- → Les attaques par DDoS visent principalement à nuire à la réputation de leur victime, à travers la médiatisation d'incidents aux conséquences majoritairement limitées à la disponibilité de leurs services
- → En 2025, cependant, les entités visées ont dû faire face à des attaques d'une envergure croissante, réalisées sur des temps courts, rendant complexes la qualification de l'attaque et la limitation de ses effets



MAINTIEN D'UN BRUIT DE FOND CONTINU PAR DES ACTEURS MALVEILLANTS

ATTAQUES PAR DÉNI DE SERVICE DISTRIBUÉ (DDOS)

- Les attaques par DDoS visent principalement à nuire à la réputation de leur victime, à travers la médiatisation d'incidents aux conséquences majoritairement limitées à la disponibilité de leurs services
- En 2025, cependant, les entités visées ont dû faire face à des attaques d'une envergure croissante, réalisées sur des temps courts, rendant complexes la qualification de l'attaque et la limitation de ses effets

Tendances générales observées

Du téléphone jusqu'au Cloud

Attaques hybrides et impacts sur infrastructures

- Augmentation des attaques destructives, notamment contre les infrastructures électriques en Pologne, illustrant le risque pour l'UE et la France.
- Les attaques hybrides combinent cyber et autres moyens, visant à provoquer des coupures et perturbations majeures.

Cloud : nouveaux vecteurs de compromission

- Adoption massive du cloud expose à des compromissions, exfiltrations de données et chiffrement de ressources, affectant services publics et privés.
- Les vulnérabilités sur équipements de bordure et l'accès aux environnements cloud sont exploités par les attaquants.

Ciblage des mobiles et prolifération offensive

- Les environnements mobiles, personnels et professionnels, sont ciblés par des capacités sophistiquées, souvent issues de sociétés privées.
- La prolifération de ces outils augmente le niveau global de la menace et facilite l'accès à un large panel d'utilisateurs.

Ciblage des mobiles

Une menace en hausse

Vulnérabilités critiques sur mobiles

- Failles exploitées dans iOS, Android, WhatsApp, Samsung
- Mises à jour publiées en 2025 pour CVE-2025-43300, CVE-2025-21043, CVE-2025-55177

Attaques zéro-clic

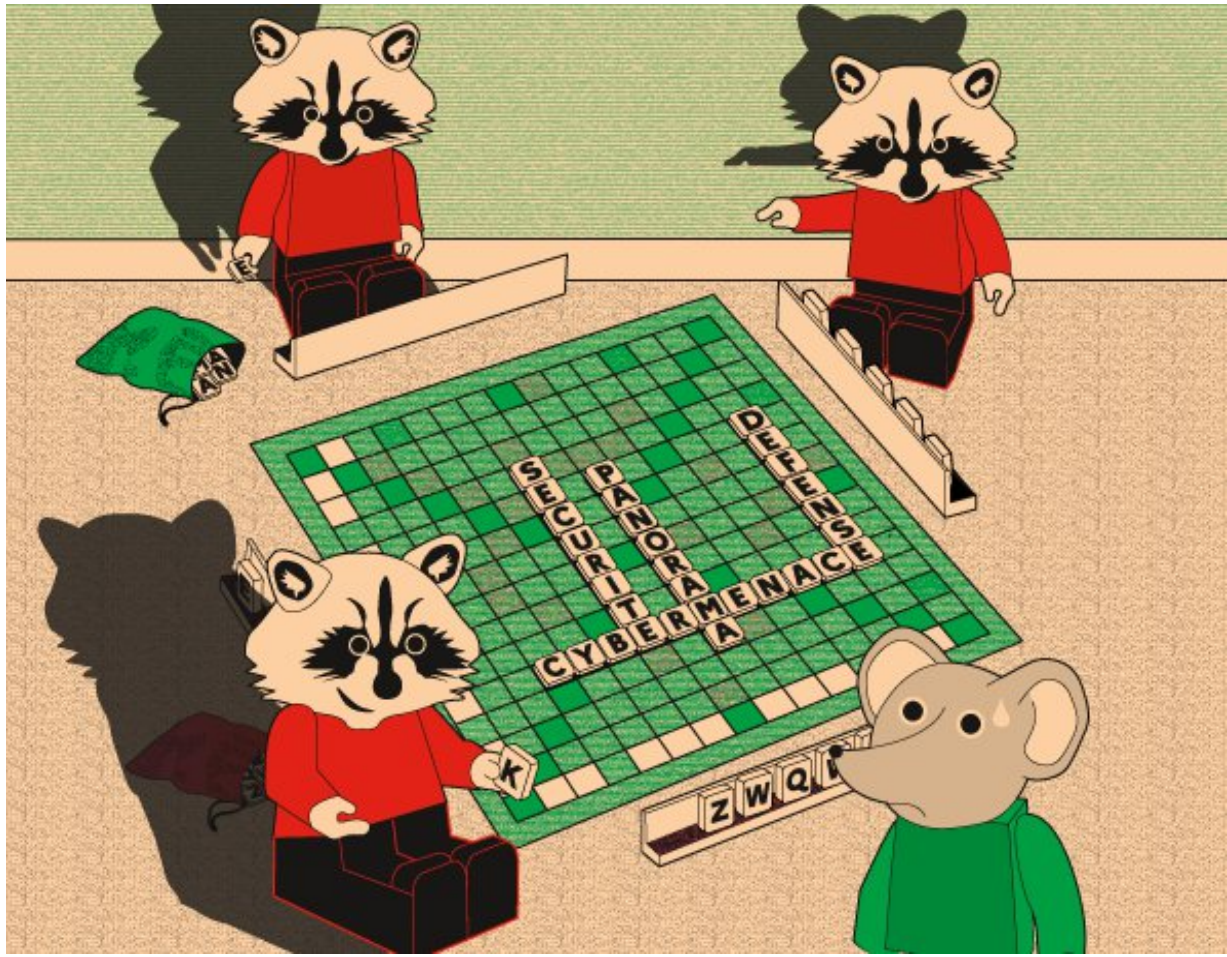
- Compromission à distance sans action de l'utilisateur
- Chaînage de vulnérabilités pour prise de contrôle totale

Espionnage et surveillance avancée

- Logiciels espions comme Pegasus, Predator, Triangulation ciblent des mobiles
- Notifications de menace envoyées par Apple depuis 2021

Ciblage massif et sophistication

- Vol de données personnelles et professionnelles
- Capacités de recherche sophistiquées pour cibler un large panel d'utilisateurs



Attaques sur la chaîne d’approvisionnement

Nécessité de renforcer l’ensemble

Compromission de prestataires

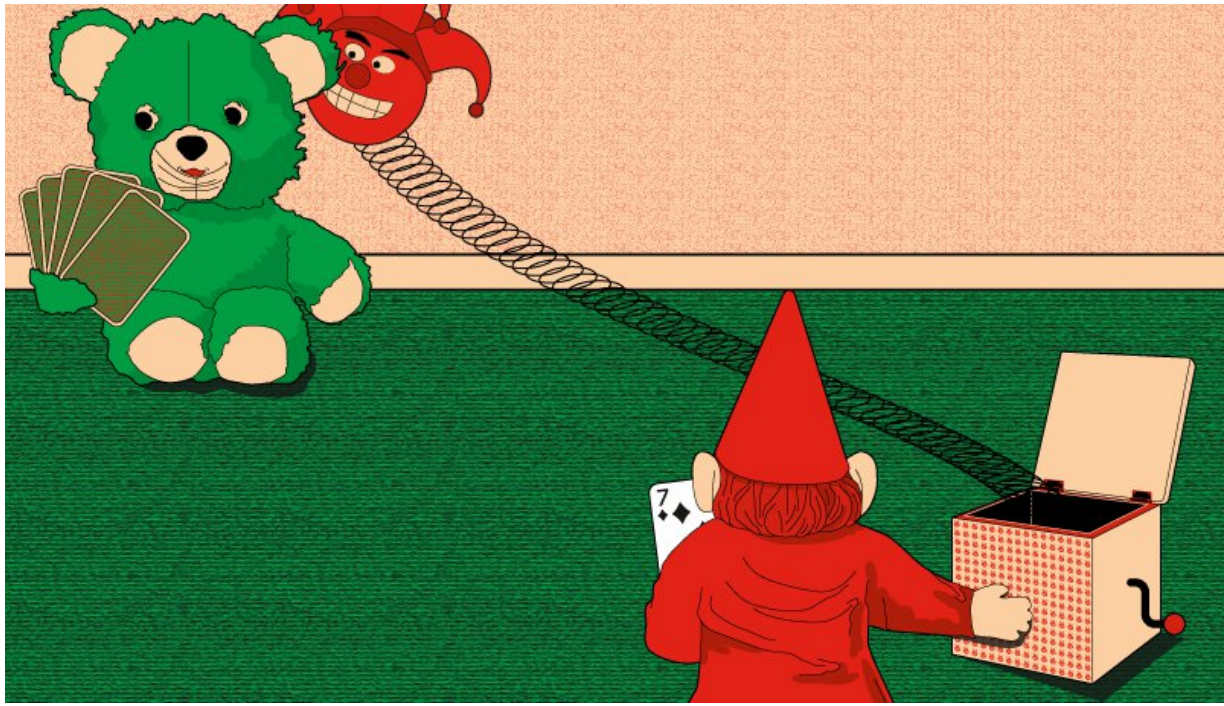
- Les attaquants ciblent les fournisseurs pour accéder aux clients.
- Latéralisation possible vers de nombreux clients via interconnexions SI.

Impacts sur secteurs critiques

- BITD, cloud, santé et collectivités touchés par des attaques en chaîne.
- Perturbation de services, vol de données, atteinte à l'image.

Difficultés d’analyse et remédiation

- Manque de contrôle sur les environnements cloud limite la réponse aux incidents.
- Accès aux logs et ressources cloud parfois insuffisant pour l’investigation.



Déstabilisation et sabotage

Les attaquants brouillent les frontières entre cybercriminalité, déstabilisation et sabotage.

Attaques destructives en Ukraine et Pologne

- Sabotages coordonnés contre infrastructures électriques polonaises en 2025, inspirés des attaques russes en Ukraine.
- Utilisation de codes destructeurs (wipers) pour viser secteurs critiques : énergie, agriculture, ferroviaire.

Sabotage de petites installations industrielles

- Multiples signalements relatifs au ciblage d'entités du secteur de la production d'énergie renouvelable par des groupes hacktivistes.
- Les attaques traitées par l'ANSSI en 2025 n'ont pas eu d'effet physique majeur.
- Actions sur vannes et turbines avec des impacts limités mais fortement médiatisés.

DDoS et médiatisation par hacktivistes pro-russes

- Multiplication des attaques par déni de service (DDoS) en France et Europe, souvent revendiquées sur Telegram.
- Objectif : nuire à la réputation, exagérer les conséquences réelles, maximiser la portée médiatique.

Ingénierie sociale et techniques avancées

Convergence des modes opératoires

Techniques d'ingénierie sociale avancées

- SIM-Swapping : transfert frauduleux de numéro pour contourner l'authentification.
- MFA Fatigue : bombardement de demandes d'authentification pour pousser la victime à accepter.
- Hameçonnage vocal : usurpation d'identité par téléphone pour obtenir des accès ou informations.

Usurpation d'identité et reconnaissance approfondie

- Collecte de données personnelles pour personnaliser les attaques.
- Imitation du support informatique pour inciter au téléchargement d'outils malveillants.

Technique Clickfix et campagnes ciblées

- Incitation à exécuter soi-même des commandes malveillantes (Clickfix).
- Déploiement de RAT et infostealers via faux captchas ou instructions personnalisées.

Vulnérabilités exploitées en 2025

Le jour même où le correctif est publié.

Cycle de vie des vulnérabilités

- La menace augmente dès la découverte d'une vulnérabilité, surtout si un code d'exploitation est rapidement publié.
- L'application rapide des correctifs est essentielle pour limiter les risques.

Vulnérabilités majeures exploitées en 2025

- Équipements Ivanti (VPN, Endpoint Manager) ciblés par plusieurs failles critiques.
- Fortinet : exploitation de failles d'authentification sur les pare-feu.
- Microsoft Sharepoint : vagues d'exploitation de vulnérabilités "toolshell" en jour-zéro.
- VMware ESXi, Workstation, Fusion : vulnérabilités critiques exploitées dès leur publication.

Faiblesses techniques et interfaces exposées

- Exposition des interfaces d'administration sur Internet reste fréquente et dangereuse.
- Des attaquants corrigent parfois eux-mêmes les failles après exploitation pour masquer leur présence.

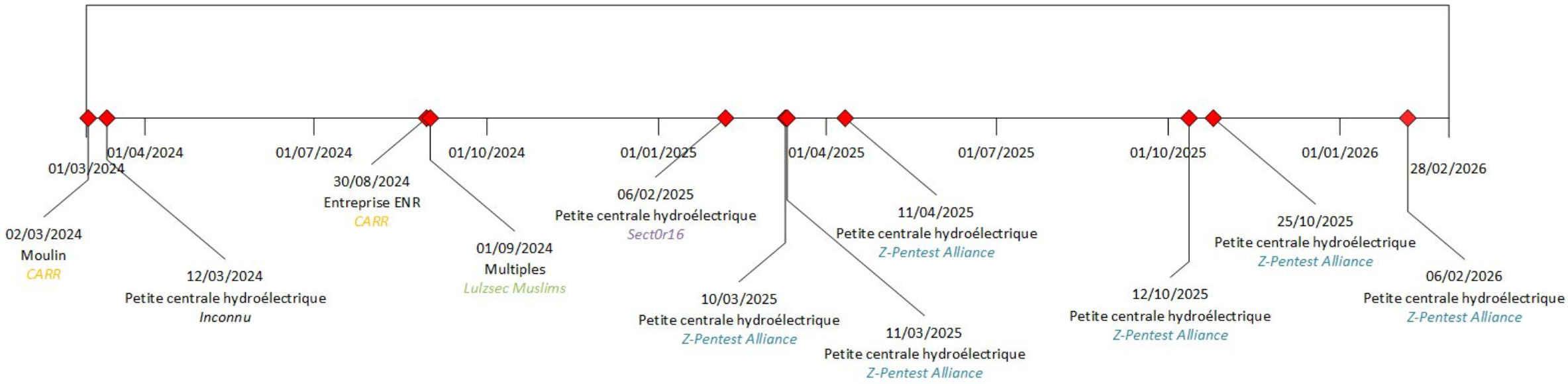
03.

Ciblage de la production d'Énergie électrique et du secteur de l'eau en France

Constats et recommandations

Contexte

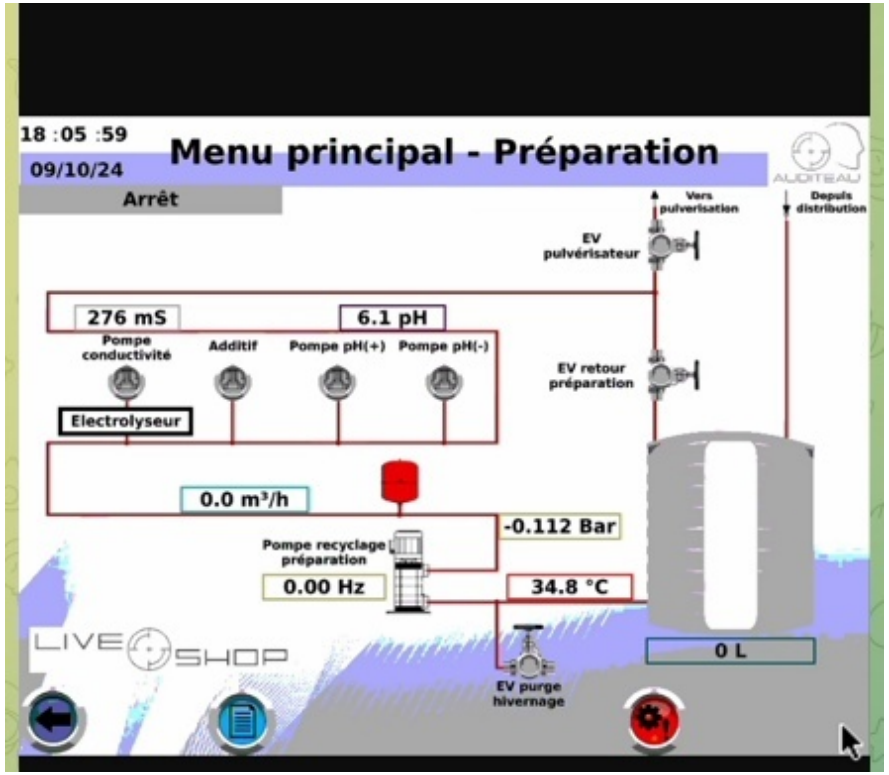
Un ciblage constant

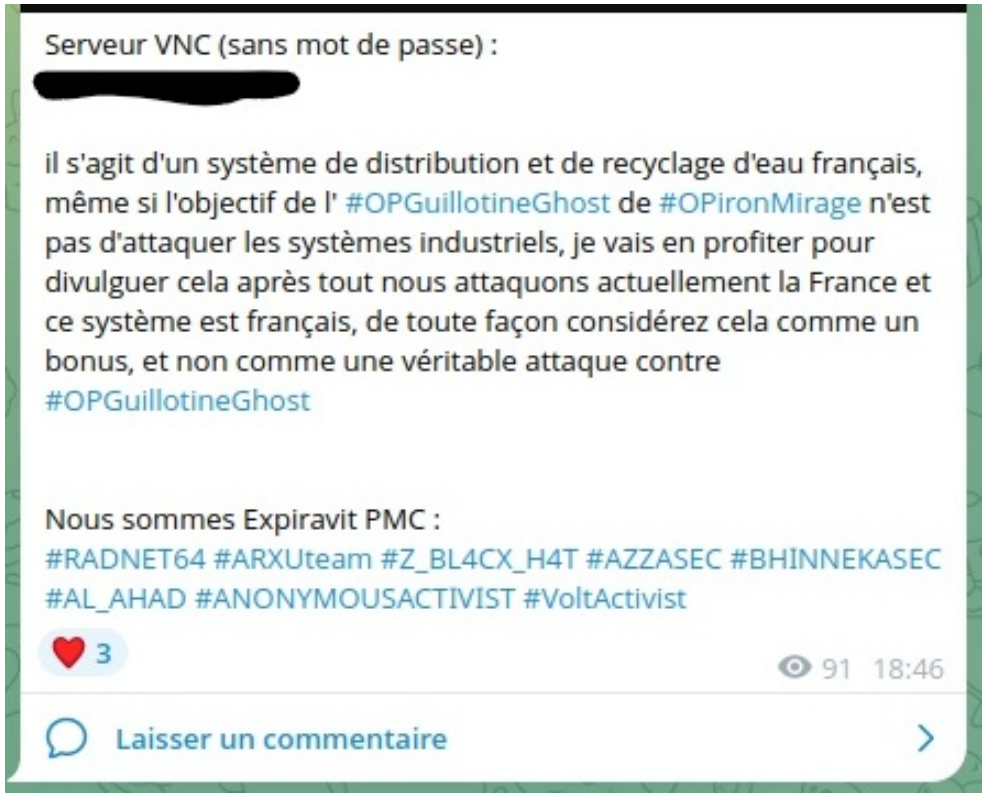


Difficultés dans la prise en compte

- Multitudes d'acteurs
- Profil des victimes (TPE, particuliers)
- Mauvaise maitrise de leur SI : recours à des intégrateurs, prestataires, etc.
- Mauvaises pratiques : accessibilité privilégiée par rapport à la sécurité
- Epuisement des ressources de l'ANSSI

Les groupes hacktivistes, menace la plus visible





Des entités plus critiques déjà ciblé chez nos partenaires

IMAGE: LENNY THIEULEUX VIA UNSPLASH

Alexander Martin
December 11th, 2023

News | Government | Cybercrime

Two-day water outage in remote Irish region caused by pro-Iran hackers

Residents of a remote area on Ireland's west coast were left without water last week due to a cyberattack perpetrated by a pro-Iran hacking group targeting a piece of equipment the hackers complained was made in Israel.

Il faut se préparer !

Constats

- Dans la plupart des cas traités par l'ANSSI, l'attaque n'est possible qu'en raisons de mauvaises pratiques
- L'ANSSI observe de nombreux équipements vulnérables et exposés sur Internet
- Difficultés à faire corriger ces mauvaises pratiques

Exposition de protocoles industriels

- Plusieurs centaines d’équipements qui supportent Modbus
- Beaucoup de petits producteurs d’énergie
- Plusieurs centaines d’équipements BACnet
- Mais aussi beaucoup d’autres protocoles
  - Ethernet/ip, FINS, CODESYS, OPC-UA, IEC-104

Exposition d’interfaces web

- Exposition de nombreuses interfaces d’administration ou de supervision
  - Automates (Schneider, Siemens, ABB, Honeywell, Niagara, Wago, Creston, RedLion, Ewon, Unitronics…)
  - Logiciels de GTB
  - Panneaux solaires/centrales photovoltaïques
  - Éoliennes
  - Hydroélectrique
  - …
- La robustesse de ces interfaces n’est pas garantie
- VNC vers des IHM
  - Souvent authentification absente ou mots de passe communs
- Caméras avec flux en clair

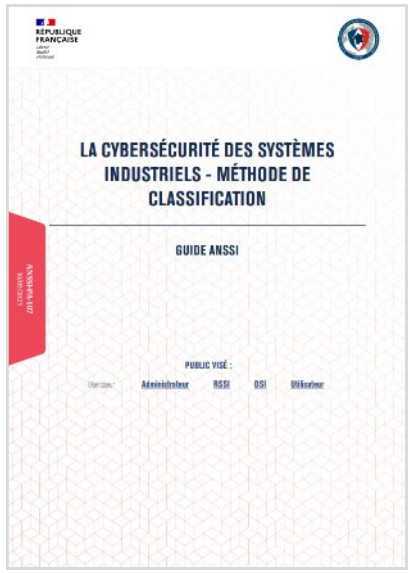
Que faire

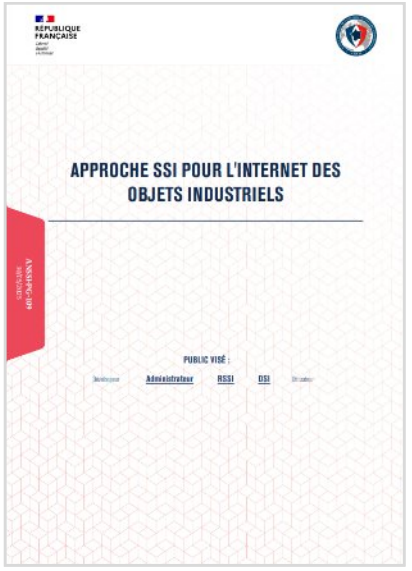
Recommandations minimales pour les PME/ETI

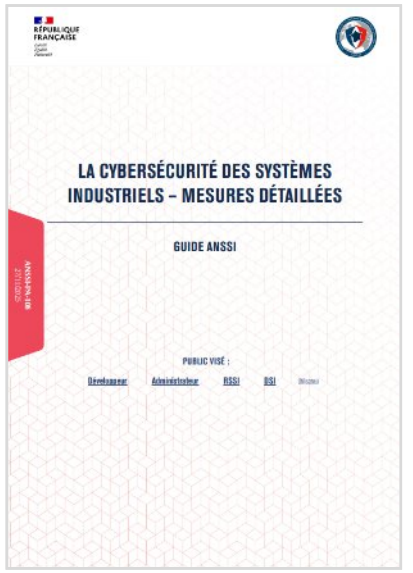
1. Mettre en œuvre un filtrage sur l'adresse IP source des équipements et des applications autorisées à se connecter à l'installation ;
2. Sécuriser l'accès à l'installation industrielle via la mise en œuvre d'un tunnel VPN IPsec ou VPN TLS.
3. Vérifier les comptes existants et remplacer l'ensemble des mots de passe et identifiants par défaut par des mots de passe complexes et robustes.
4. Activer les options d'authentification à multiples facteurs lorsque celles-ci sont disponibles ;
5. Utiliser un logiciel d'accès distant maintenu à jour par son éditeur avec des protocoles sécurisés, standardisés et éprouvés (TLS ou SSH) ;
6. Appliquer les correctifs de sécurité côté client et serveur dans les meilleurs délais.

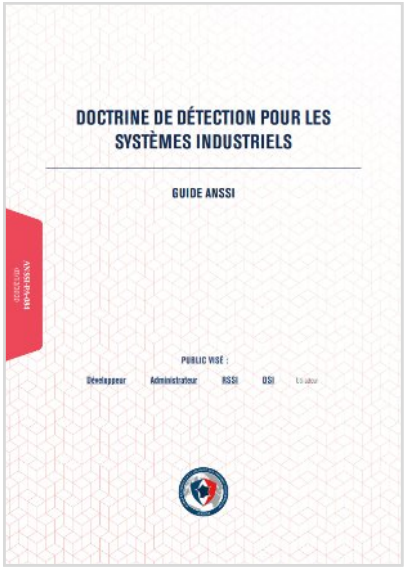
Publication à retrouver ici : Recommandations à destination des acteurs du secteur de l'énergie et de l'eau - CERT-FR

Pour aller plus loin









Plus de ressources sur messervices.cyber.gouv.fr

En cas de compromission

- Les bons réflexes en cas d'intrusion sur un système d'information : https://www.cert.ssi.gouv.fr/les-bons-reflexes-en-cas-dintrusion-sur-un-systeme-dinformation/

- Contactez le CERT-FR :
  - cert-fr@ssi.gouv.fr
  - 3218 ou 09 70 83 32 18

04.

NIS2 & publication du Référentiel Cyber France (ReCyF)

Retour sur l'évènement de lancement du 17 mars 2026

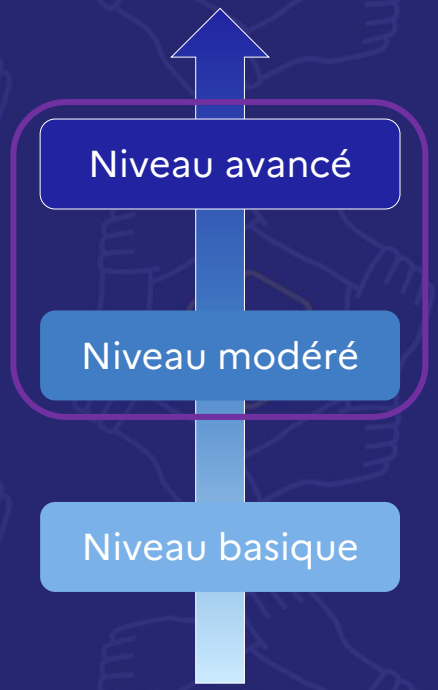
Présentation du Référentiel France

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

NIS 2

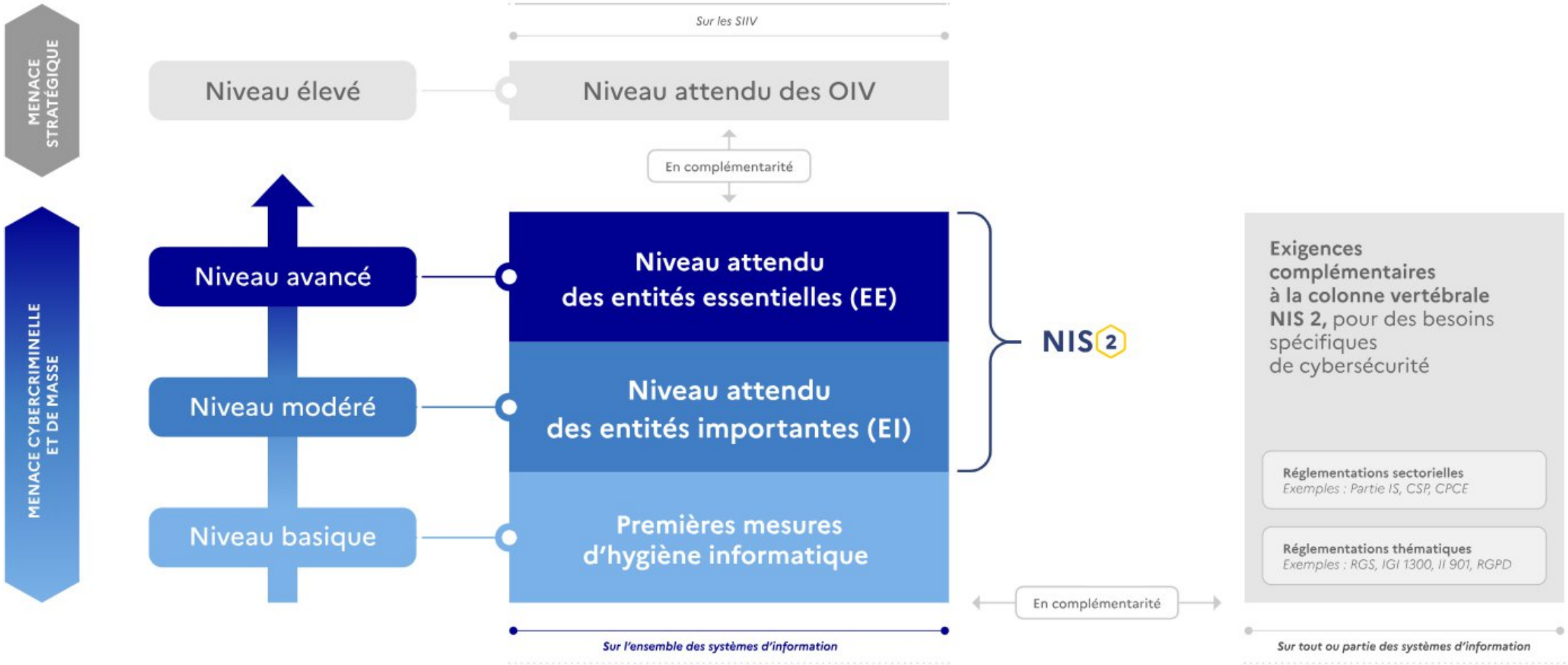
Lançons collectivement la dynamique de sécurisation

1 – Le Référentiel de Cybersécurité France – ReCyF



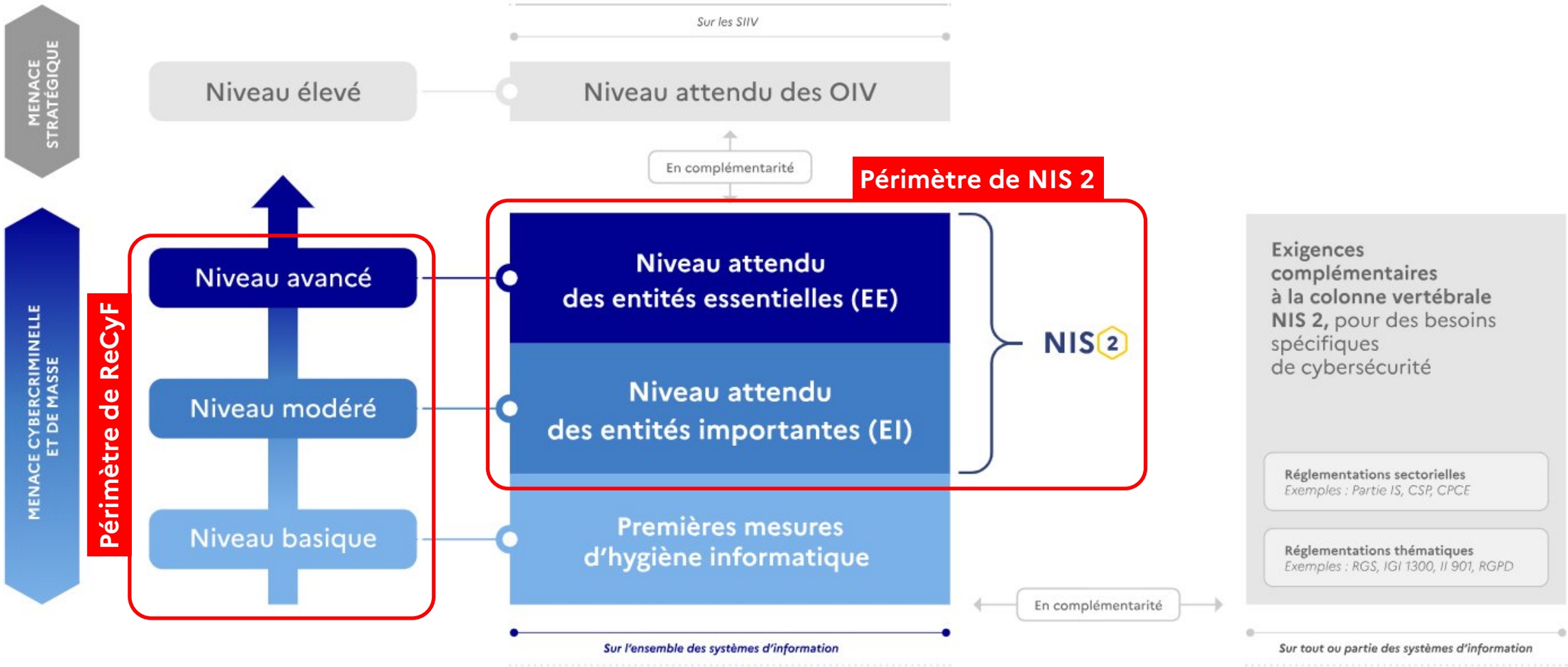
NIS 2 comme colonne vertébrale du cadre règlementaire de cybersécurité

④ **Trois niveaux de mesures de sécurité** autour desquelles toutes les règlementations de cybersécurité ont vocation à s'articuler



NIS 2 comme colonne vertébrale du cadre règlementaire de cybersécurité

④ **Trois niveaux de mesures de sécurité** autour desquelles toutes les règlementations de cybersécurité ont vocation à s'articuler



Une approche proportionnée de l'analyse de risques

Objectifs de l'analyse des risques

- **Prioriser** les exigences de sécurité et **adapter** les modalités de leur mise en oeuvre à la taille de l'entité, son organisation et la complexité de son SI
- **Identifier** les mesures complémentaires aux mesures d'hygiène nécessaires à l'entité pour qu'elle se protège efficacement et de manière pérenne contre des menaces qui lui sont spécifiques

Adapter les mesures en fonction du risque auquel on fait face

Approche proportionnée et mise en oeuvre différenciée

Pour les entités importantes (EI) — RÉALISÉE PAR L'ANSSI

Approche par conformité : Identification par l'ANSSI des risques génériques pour les EI

Pourquoi : Une typologie d'entités en majorité peu matures, avec peu de ressources et une démarche cyber insuffisante

Comment : Application des mesures concrètes du référentiel dans une logique de « conformité/ check list »

Pour les plus matures — RECOMMANDÉ

Adopter l'approche EE et réaliser une analyse des risques

Pour les entités essentielles (EE) — OBLIGATOIRE

Approche par conformité : Réalisation par l'entité de son analyse de risques spécifiques

Pourquoi : Une typologie d'acteurs en majorité matures et généralement déjà régulés

Comment : Obligation de réaliser une analyse de risques afin d'adapter la mise en oeuvre des mesures de sécurité et d'identifier les besoins complémentaires de sécurisation

Les quatre piliers essentiels des mesures de cybersécurité (1/2)

20 objectifs pour 4 piliers (Gouvernance, Défense, Protection, Résilience), Dont certains sont spécifiques aux futures EE

(7 objectifs)

- Recensement des SI
- Mise en œuvre d'un cadre de gouvernance de la sécurité numérique
- Maîtrise de l'écosystème (prestataires et fournisseurs informatiques)
- Prise en compte de la sécurité numérique dans la gestion des ressources humaines
- Maîtrise des SI
- Mise en œuvre d'une approche par les risques
- Audit de la sécurité des SI

→ Objectifs spécifiques aux entités essentielles (EE)

(2 objectifs)

- Identification et réaction aux incidents de sécurité
- Supervision de la sécurité des SI

→ Objectif spécifique aux entités essentielles (EE)

Les quatre piliers essentiels des mesures de cybersécurité (2/2)

(8 objectifs)

- Maitrise des accès physiques aux locaux
- Sécurisation de l'architecture des SI
- Sécurisation des accès distants aux SI
- Protection des SI contre les codes malveillants
- Gestion des identités et des accès des utilisateurs aux systèmes
- Maîtrise de l'administration des SI
- Sécurisation de la configuration des ressources des SI
- Administration des SI depuis des ressources dédiées

Objectifs spécifiques aux entités essentielles (EE)

(3 objectifs)

- Continuité et reprise d'activité
- Réaction aux crises d'origine cyber
- Exercices, tests et entraînements

Pour répondre à ces objectifs de sécurité, l'ANSSI propose un référentiel d'exigences : ReCyF

Le Référentiel ReCyF

PROPORTIONNALITÉ

Pour se défendre contre la menace cybercriminelle de masse :

- **20 objectifs** de sécurité pour les entités essentielles (EE)
- **15 objectifs** de sécurité pour les entités importantes (EI), correspondant à des mesures d'hygiène numérique

NIS 2 – TRANSPOSITION NATIONALE

MESURES DE GESTION DES RISQUES EN MATIÈRE DE CYBERSECURITÉ

RECYF :

RÉFÉRENTIEL CYBER FRANCE

(ReCyF)

Version 2.5 du 17/03/2026

VERSION DE TRAVAIL

OBJECTIFS DE SECURITE APPLICABLES AUX ENTITÉS IMPORTANTES ET ESSENTIELLES

GOUVERNANCE DES SYSTEMES D'INFORMATION

OBJECTIF DE SÉCURITÉ 1. RECENSEMENT DES SYSTEMES D'INFORMATION

Objectif de sécurité

RAPPEL DE L'OBJECTIF DE SECURITE

Les entités [importantes ou essentielles] réalisent et maintiennent à jour une liste de l'ensemble de leurs activités et services ainsi que des systèmes d'information y contribuant.

Ces entités sont tenues d'appliquer les [objectifs de sécurité] sur l'ensemble de leurs systèmes d'information, à l'exception de ceux pour lesquels elles justifient, sur la base d'une analyse de risques, qu'ils ne sont pas exposés à l'un des risques suivants :

1. La dégradation ou l'interruption, directe ou indirecte, des activités ou services de l'entité ;
2. La divulgation à des personnes non autorisées d'informations sensibles traitées par les activités ou services de l'entité ;
3. L'altération des informations nécessaires aux activités ou services de l'entité.

La mise en œuvre de mesures de sécurité sur ces systèmes d'information ne permet pas de justifier qu'ils ne sont exposés à aucun des risques précités.

Pour ces systèmes d'information, le choix de ne pas appliquer les objectifs de sécurité ainsi que sa justification au regard des critères précédents doivent apparaître explicitement dans la liste mentionnée au premier alinéa.

MOYENS ACCEPTABLES DE CONFORMITE

		ATTENDU D'UNE EI	ATTENDU D'UNE EE
1.1-EI/EE	L'entité liste l'ensemble de ses activités et services, y compris les activités et services qui ne correspondent pas aux critères pour lesquels l'entité constitue une entité importante ou essentielle (*par exemple : une entité essentielle au titre d'une activité exploitation d'un oléoduc doit lister, en plus des activités et services participant à l'exploitation de l'oléoduc, tous les services et les autres activités qu'elle fournit*). Pour chaque entrée de cette liste, l'entité : o identifie un responsable de l'activité ou du service (*par exemple le chef de service auquel est rattachée l'activité ou le service, un directeur métier, la direction générale*) ; o liste les systèmes d'information les supportant.	Oui	Oui
1.2-EI/EE	L'entité précise dans la liste prévue au 1.1-EI/EE les systèmes d'information qui ne sont exposés à aucun des risques mentionnés à l'alinéa 2 de l'objectif de sécurité. L'entité renseigne les justifications de ces choix.	Oui	Oui
1.3-EI/EE	L'entité valide et réexamine annuellement la liste prévue au 1.1-EI/EE, et en tant que de besoin, notamment en cas d'évolution des activités et services de l'entité ou en cas de mise en service d'un nouveau système d'information.	Oui	Oui

Exigences : « comment l'atteindre »

Prochaines étapes du ReCyF

Publication depuis le 17 mars sur MesServicesCyber :

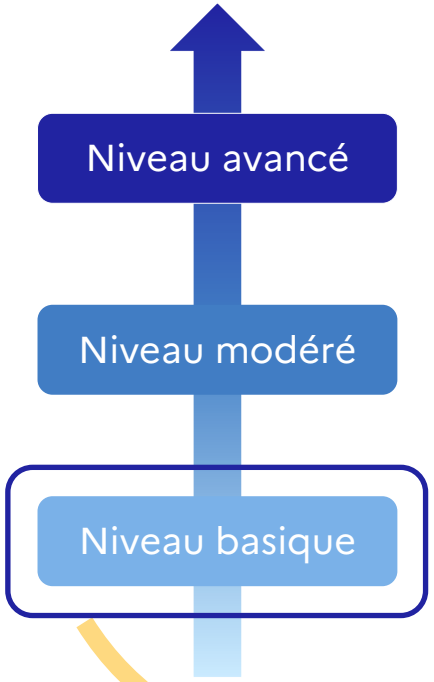
- La dernière version du référentiel 2.5 en date de mars 2026 ;
- L'analyse d'écart par rapport à la version 2.4.

Cette publication n'est pas un appel à contribution. Une consultation sur le référentiel sera réalisée préalablement à la publication des décrets d'application du projet de loi Résilience (PJL).

Le référentiel présenté demeure une version « beta » provisoire, donc susceptible d'évoluer en fonction des travaux législatifs et réglementaires.

Le niveau basique

Non obligatoire : le niveau basique de ReCyF sera fourni comme une aide « pour démarrer »



Le niveau basique se compose d'un **sous-ensemble de mesures du référentiel ReCyF actionnables** facilement et rapidement pour les entités les moins matures.

Chaque mesure a pour objectif de générer un **impact rapide de sécurisation** face aux menaces systémiques les plus rencontrées.

Une première version du niveau basique sera publiée dans les prochaines semaines sur MesServicesCyber.

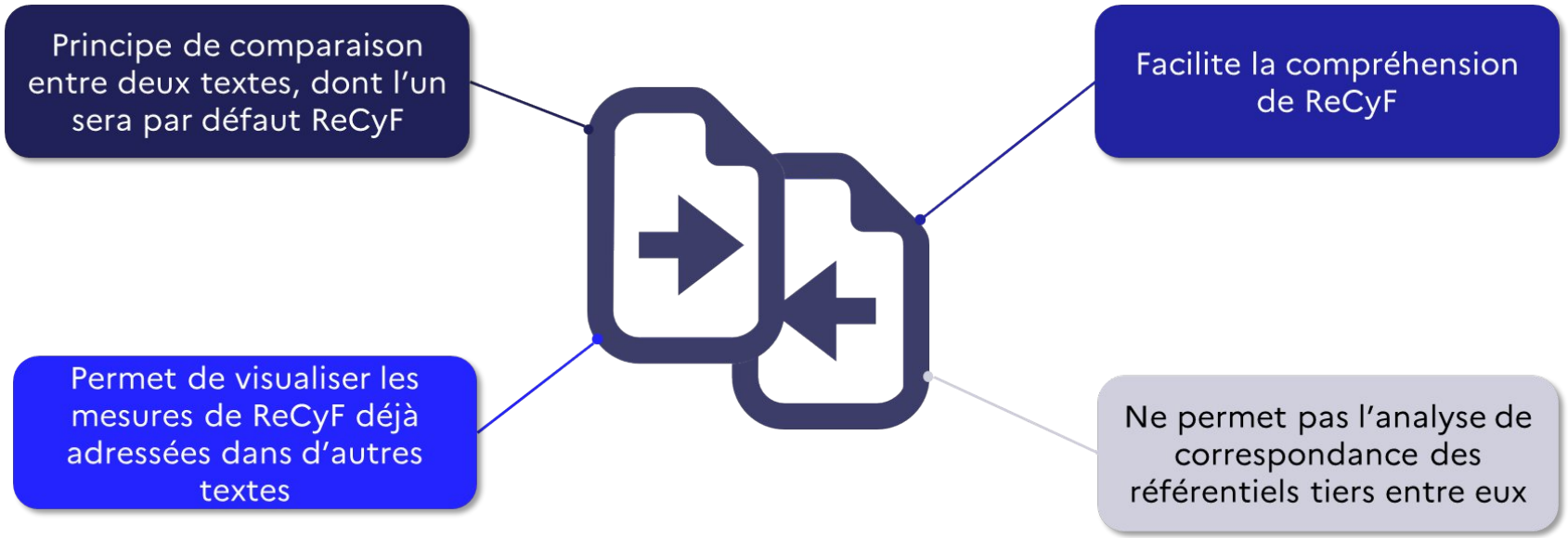
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

NIS 2

2 – Outil de comparaison des référentiels

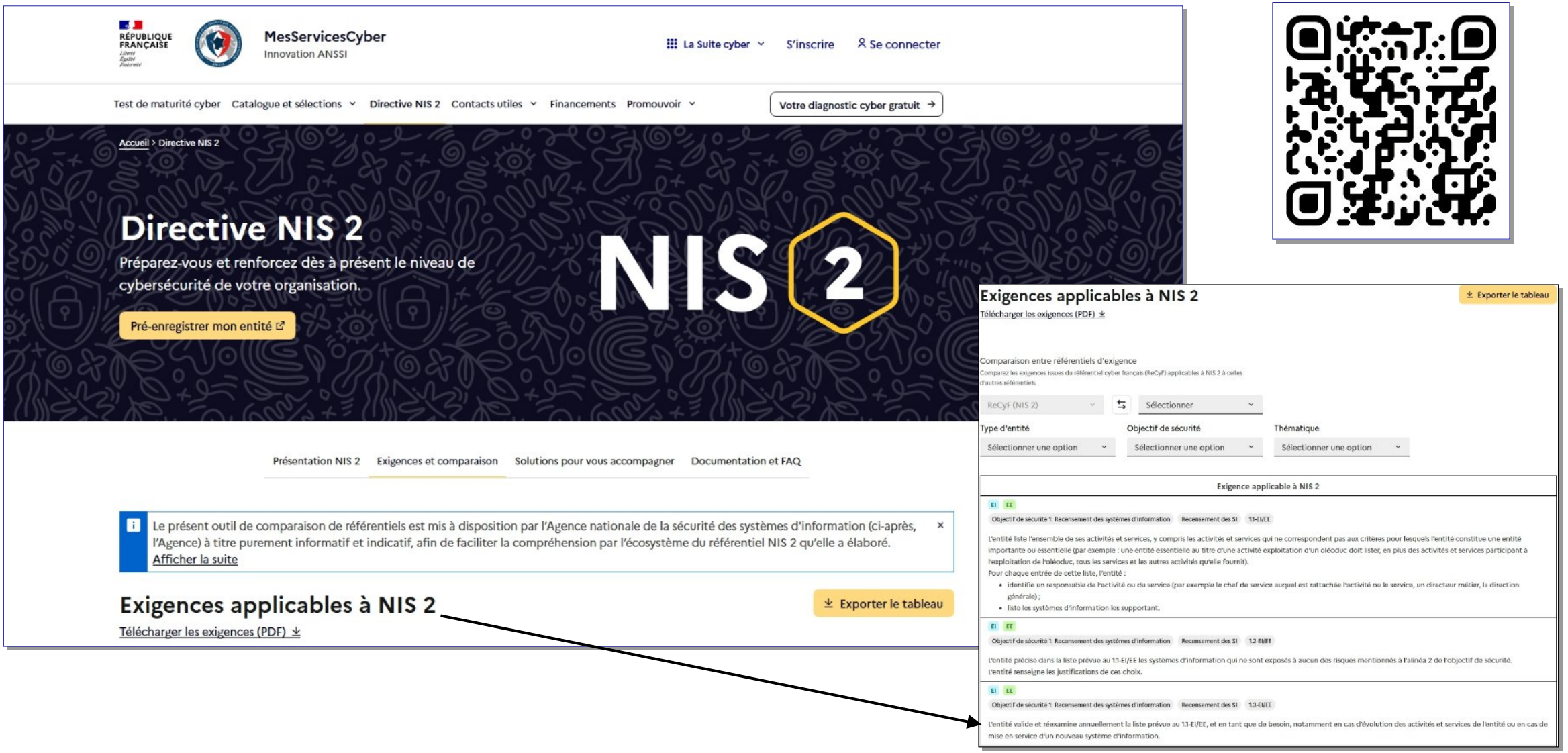
Objectifs de l'outil de comparaison des référentiels

④ L'outil de comparaison s'inscrit dans un objectif global d'**harmonisation des référentiels de sécurité** et vise à mieux comprendre ReCyF et l'esprit de ses exigences.



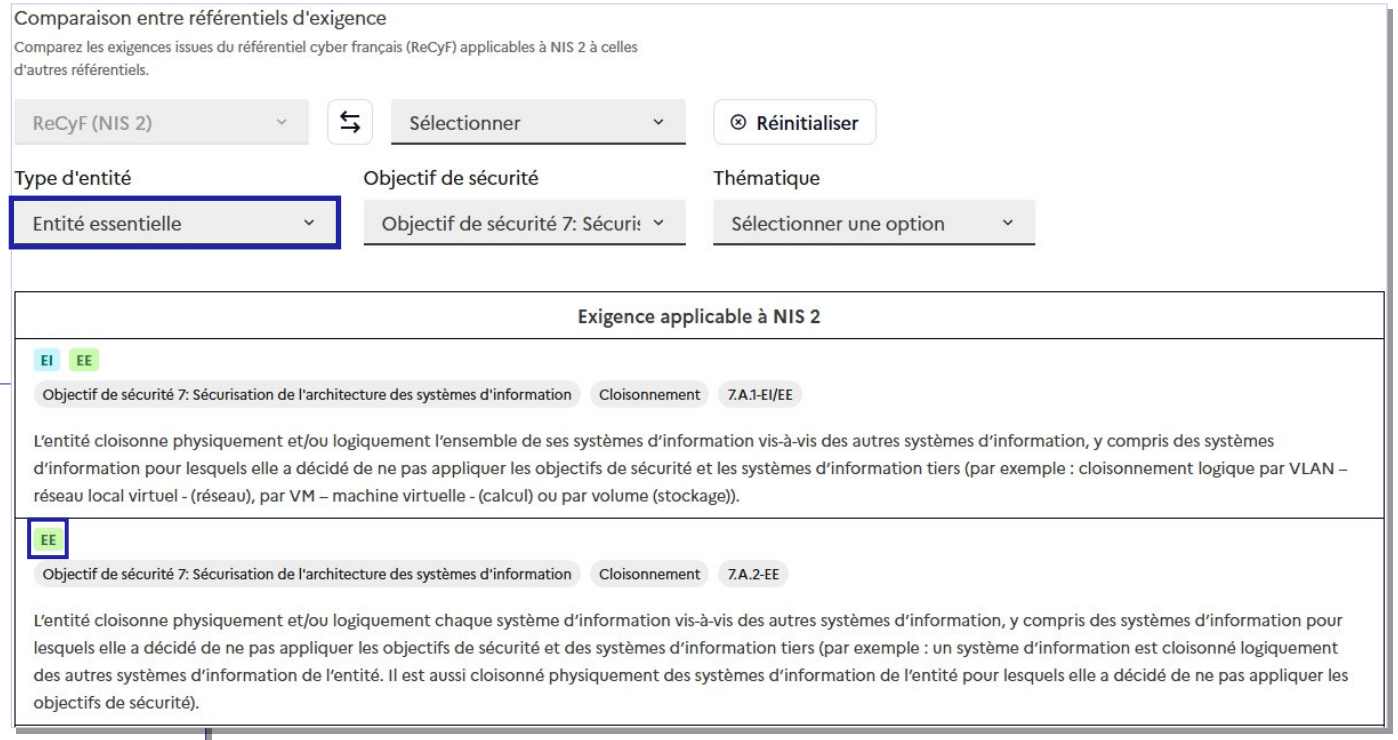
- L'outil est à titre purement **informatif** et **indicatif ;**
- Les analyses présentées **ne sauraient être interprétées comme des prescriptions** à l'égard des entités ;
- Son utilisation est **sans préjudice** de l'appréciation qui pourrait être portée par l'ANSSI dans le cadre de son **activité de supervision et de contrôle** ;
- Il ne **constitue en aucun cas** une **décision de reconnaissance des autres référentiels** comme prévu dans le **PJL Résilience.**

Présentation de l'outil (1/3)

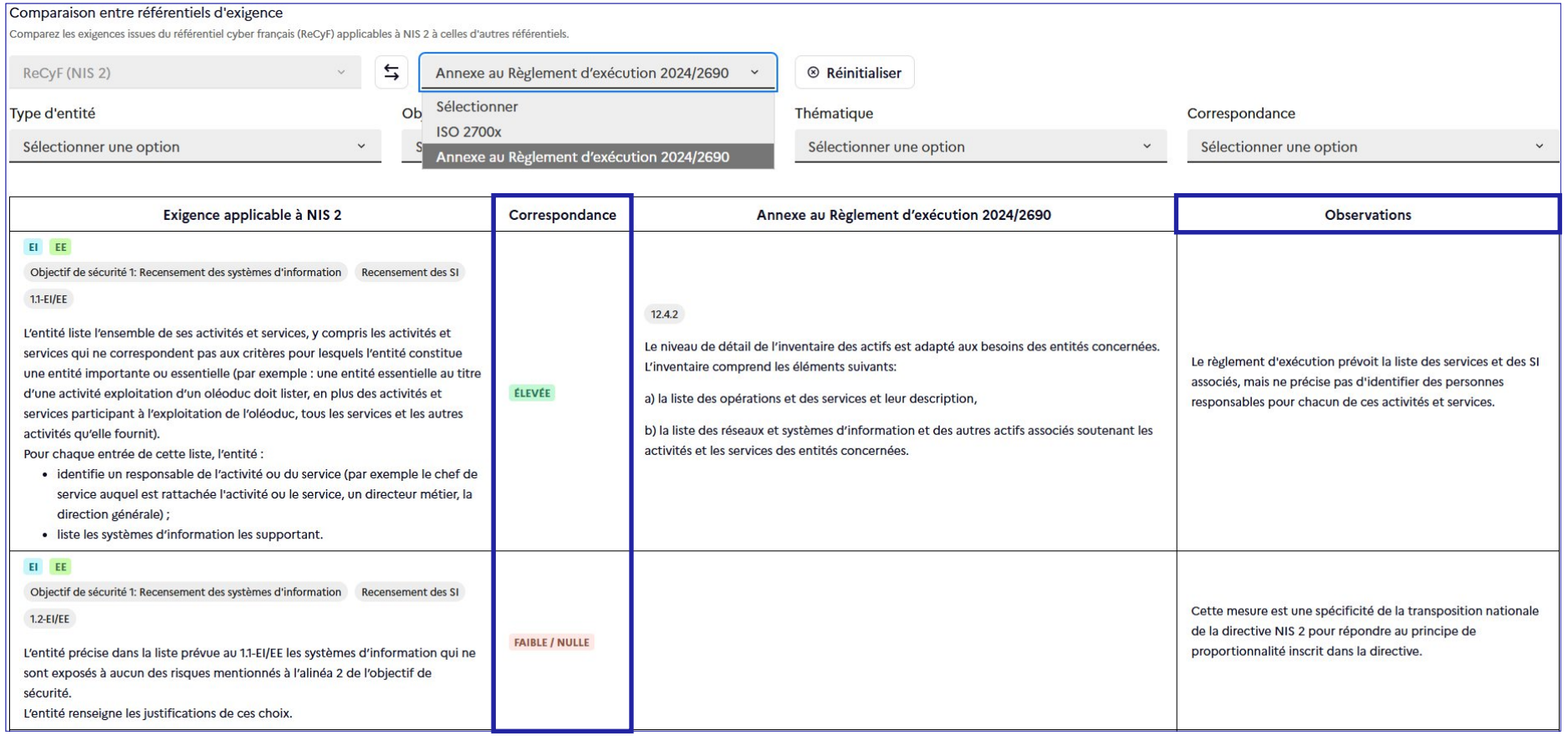


Présentation de l'outil (2/3)

Distinction entre les exigences à destination des entités importantes et essentielles



Présentation de l'outil (3/3)



Comparaison entre référentiels d'exigence

Comparez les exigences issues du référentiel cyber français (ReCyF) applicables à NIS 2 à celles d'autres référentiels.

ReCyF (NIS 2) ⇆ Annexe au Règlement d'exécution 2024/2690 ⊗ Réinitialiser

Sélectionner
ISO 2700x
Annexe au Règlement d'exécution 2024/2690

Type d'entité: Sélectionner une option

Thématique: Sélectionner une option

Correspondance: Sélectionner une option

Exigence applicable à NIS 2	Correspondance	Annexe au Règlement d'exécution 2024/2690	Observations
EI EE Objectif de sécurité 1: Recensement des systèmes d'information — Recensement des SI 1.1-EI/EE L'entité liste l'ensemble de ses activités et services, y compris les activités et services qui ne correspondent pas aux critères pour lesquels l'entité constitue une entité importante ou essentielle (par exemple : une entité essentielle au titre d'une activité exploitation d'un oléoduc doit lister, en plus des activités et services participant à l'exploitation de l'oléoduc, tous les services et les autres activités qu'elle fournit). Pour chaque entrée de cette liste, l'entité : • identifie un responsable de l'activité ou du service (par exemple le chef de service auquel est rattachée l'activité ou le service, un directeur métier, la direction générale) ; • liste les systèmes d'information les supportant.	ÉLEVÉE	12.4.2 Le niveau de détail de l'inventaire des actifs est adapté aux besoins des entités concernées. L'inventaire comprend les éléments suivants: a) la liste des opérations et des services et leur description, b) la liste des réseaux et systèmes d'information et des autres actifs associés soutenant les activités et les services des entités concernées.	Le règlement d'exécution prévoit la liste des services et des SI associés, mais ne précise pas d'identifier des personnes responsables pour chacun de ces activités et services.
EI EE Objectif de sécurité 1: Recensement des systèmes d'information — Recensement des SI 1.2-EI/EE L'entité précise dans la liste prévue au 1.1-EI/EE les systèmes d'information qui ne sont exposés à aucun des risques mentionnés à l'alinéa 2 de l'objectif de sécurité. L'entité renseigne les justifications de ces choix.	FAIBLE / NULLE		Cette mesure est une spécificité de la transposition nationale de la directive NIS 2 pour répondre au principe de proportionnalité inscrit dans la directive.

Plusieurs niveaux de correspondance

- **Rouge** : aucune correspondance
- **Orange** : correspondance partielle, spécificités présentes dans un des documents
- **Vert** : correspondance acceptable, des divergences mineures peuvent subsister

Commentaires expliquant les niveaux de correspondance attribués et les deltas entre les mesures associées le cas échéant

Quels sont les référentiels disponibles ?

Ce qui est mis à disposition à date

- **Comparaisons avec l'ISO 27001 et 27002**
- Comparaison avec l'annexe du Règlement d'exécution 2024/2690, à destination notamment des ESN

Prochains référentiels comparés avec ReCyF

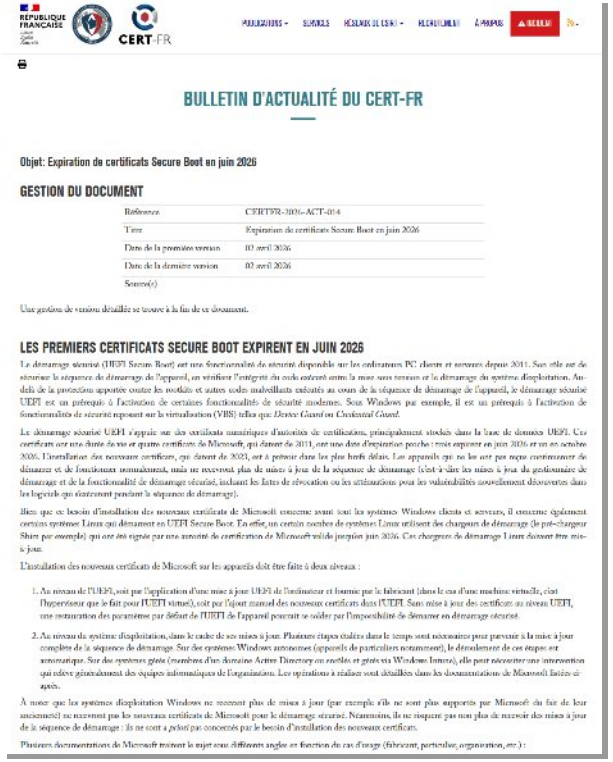
- Ajout de comparaisons au fil de l'eau
- En cours : le référentiel belge « CyFun 2023 »
- A venir : CyFun 2025, DORA, NIST Cybersecurity Framework, AirCyber, RMC

05.

Actus Cyber

Bulletin d'actualité du CERT-FR – 2 Avril 2026

CERTFR-2026-ACT-014



BULLETIN D'ACTUALITÉ DU CERT-FR

Objet: Expiration de certificats Secure Boot en juin 2026

GESTION DU DOCUMENT

Référence	CERTFR-2026-ACT-014
Titre	Expiration de certificats Secure Boot en juin 2026
Date de la première version	02 avril 2026
Date de la dernière version	02 avril 2026
Source(s)	

Une gestion de version détaillée se trouve à la fin de ce document.

LES PREMIERS CERTIFICATS SECURE BOOT EXPIRENT EN JUIN 2026

- **Expiration prochaine (entre 24 juin et 10 octobre 2026) des certificats intégrés dans la majorité des appareils.**

- **Périmètre impacté**
  - **Postes de travail, serveurs, hyperviseurs et machines virtuelles** Windows et Linux.
  - Certains chargeurs Linux (ex. **Shim**) signés par Microsoft doivent être mis à jour.

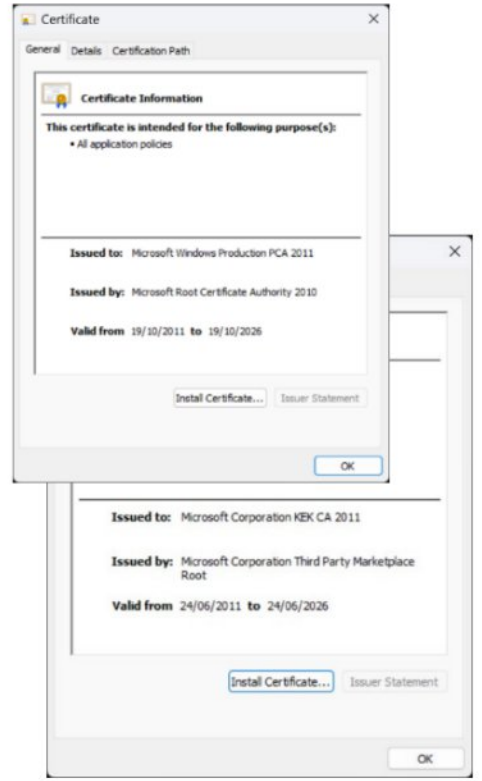
- **Conséquences si non mise à jour**
  - Les appareils **démarrent toujours**, mais **n'appliquerons plus** : mises à jour du gestionnaire de démarrage, listes de révocation, et mitigations de vulnérabilités liées au boot.
  - Sans certificats à jour, le démarrage en Secure Boot ne pourra pas se faire sur les systèmes d'exploitation signés après le 19 octobre 2026.

https://www.cert.ssi.gouv.fr/actualite/CERTFR-2026-ACT-014/

Bulletin d'actualité du CERT-FR – 2 Avril 2026

CERTFR-2026-ACT-014

- **Actions recommandées (priorité avant 24 juin 2026)**
  - **Niveau UEFI** : appliquer les mises à jour firmware fournies par les fabricants ou ajouter manuellement la nouvelle chaîne de certificats (hyperviseur pour VM).
  - **Niveau OS** : déployer les mises à jour système (automatique sur postes de travail autonomes ; intervention IT pour environnements gérés).
  - **Vérifier** hyperviseurs et images VM pour propagation des certificats.
- **Message opérationnel**
  - Traiter ce sujet comme un exercice d'**agilité cryptographique** : planifier et déployer la nouvelle chaîne de certificats dans le firmware et les composants logiciels.
  - **Priorité élevée** pour les ordinateurs portables et infrastructures critiques. Mise à jour du PCA/PRA pour tenir en compte des spécificités.



Actualités Cyber

Abonnement à la revue de presse

1. Mail aux COS Energie
2. Remplir le formulaire d'adhésion
3. La revue de presse est envoyée chaque matin entre 8h et 9h à partir de sources ouvertes

Afficher dans le navigateur

RÉPUBLIQUE FRANÇAISE

ACTUALITÉS DE LA CYBERSÉCURITÉ

Revue de presse
CERT-FR
Veille et Transmission

MONDE - Alerte de Google contre une vulnérabilité jour zéro activement exploitée

03/04/2026

Selon un article de *GBHackers* du 1er avril 2026, reprenant un avis de sécurité de Google, une vulnérabilité jour zéro serait activement exploitée. Suivie en tant que CVE-2026-5281 (CVSS v3.1 : 8,8), elle serait due à un défaut de mémoire de type utilisation de mémoire après libération (use after free) dans le composant Dawn. L'exploitation de cette vulnérabilité permettrait à un éventuel attaquant d'exécuter du code arbitraire à distance (RCE) ou de déclencher des plantages du système lorsqu'une victime visite un site Internet compromis. Google aurait confirmé qu'un code d'exploitation spécifique existerait dans la nature. Cette vulnérabilité a été corrigée par Google dans la version 146.0.7680.177/.178 du navigateur pour Windows et Mac, et dans la version 146.0.7680.177 pour Linux.

- Google, 31/03/2026
- CERT-FR, 01/04/2026
- GBHackers, 01/04/2026

Mes Services Cyber

https://messervices.cyber.gouv.fr/

https://messervices.cyber.gouv.fr/catalogue#guides

Calendrier du GT

Prochaines dates (vendredis 14h-15h30) :

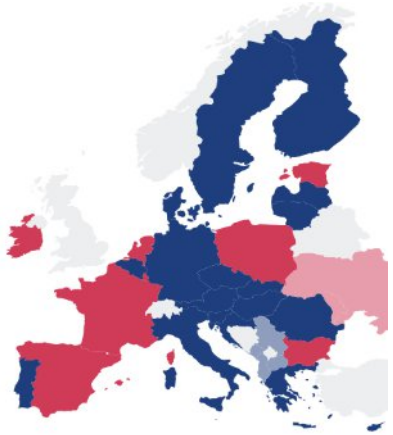
- 12 juin
- 18 sept
- 20 nov

Mailing-list : nous signaler les ajouts / retraits

Sujets à venir :

- Stratégie Nationale Cyber 2026-2030
- Les dispositifs d'accompagnement : outils « Test de maturité cyber » et « Diagnostic cyber », suites potentielles à destination des entités

Actualités Cyber



NIS2 : principales actus et pré-enregistrement NIS2

Dernières publications ANSSI

- Oct 2025 : Les Essentiels – Mise en œuvre d'un serveur Windows et de sa sécurisation
- Oct 2025 : Référentiel d'exigences applicables aux prestataires de réponse aux incidents de sécurité (PRIS) – v3.2
- Nov 2025 : Etat de la menace sur les équipements mobiles [recommandé]
- Dec 2025 : Retex sur REMPAR25
- Jan 2026 : Collection Remédiation - Préparer la remédiation
- Jan 2026 : Les Essentiels - Sécuriser sa migration informatique
- Fev 2026 : L'IA générative face aux attaques informatiques (Synthèse de la menace) [recommandé]

Publications à venir : Panorama de la cybermenace 2025 (11 mars 2026) [recommandé]