AYI NEDJIMI Consultants

Livre Blanc : Directive - Guide Pratique Cybersecurite

Catégorie : Livres Blancs Lecture : 15 min Publié le : 07/12/2025 Auteur : Ayi NEDJIMI

Découvrez notre guide détaillé sur la directive NIS 2, ses implications pour les entreprises et les stratégies de mise en conformité. Comprenez les...

Livre Blanc

La Directive NIS 2 et son Application en France : Guide Complet pour la Cybersécurité et la Résilience

Cette analyse detaillee de Livre Blanc : Directive - Guide Pratique Cybersecurite s'appuie sur les retours d'experience d'equipes de securite confrontees quotidiennement aux menaces actuelles. Les methodologies presentees couvrent l'ensemble du cycle de vie de la securite, de la detection initiale a la remediation complete, en passant par l'investigation forensique et le durcissement des configurations. Les recommandations sont directement applicables dans les environnements de production et tiennent compte des contraintes operationnelles rencontrees par les equipes techniques sur le terrain. Les outils et techniques presentes ont ete valides dans des contextes reels d'incidents et de tests d'intrusion. La mise en oeuvre d'une strategie de defense en profondeur reste essentielle face a l'evolution constante du paysage des menaces, en combinant prevention, detection et capacite de reponse rapide aux incidents de securite.

I. Introduction à la Directive NIS 2

A. Contexte et Objectifs : Pourquoi NIS 2?

La Directive (UE) 2022/2555, communément appelée NIS2 (Network and Information Security 2), constitue le cadre réglementaire européen le plus récent et le plus ambitieux visant à renforcer la cybersécurité au sein de l'Union Européenne. Son entrée en vigueur le 16 janvier 2023 marque une étape décisive dans la stratégie de l'UE pour faire face à un paysage de menaces numériques en constante évolution. L'objectif fondamental de NIS2 est d'établir un niveau commun élevé de cybersécurité pour les systèmes de réseaux et d'information, répondant ainsi à la dépendance croissante des sociétés et des économies aux technologies numériques.

La directive exige des États membres qu'ils renforcent leurs capacités nationales en matière de cybersécurité, qu'ils mettent en œuvre des mesures de gestion des risques robustes et qu'ils introduisent des obligations de notification des incidents pour un éventail élargi de secteurs considérés comme critiques. Au-delà de la simple protection des infrastructures, NIS2 vise à garantir le fonctionnement ininterrompu des services essentiels à la société et à l'économie, reconnaissant que la perturbation d'un service dans un État membre peut avoir des répercussions en cascade sur l'ensemble de l'Union.

La nécessité de NIS2 découle directement des lacunes identifiées dans sa prédécesseure, NIS1 (Directive 2016/1148), et de l'évolution rapide et complexe du paysage des cybermenaces. La directive précédente, bien que pionnière, a souffert d'une mise en œuvre hétérogène et de règles souvent ambiguës concernant la notification des incidents. Cette approche fragmentée a créé des "maillons faibles" dans l'infrastructure numérique européenne, exploitables par des acteurs malveillants. La numérisation croissante et l'interconnexion de tous les secteurs ont mis en lumière des vulnérabilités qui dépassent les frontières nationales, rendant une approche non coordonnée inefficace. NIS2 représente ainsi un impératif stratégique pour harmoniser et élever les standards de cybersécurité à l'échelle de l'Union. Il s'agit de construire un marché unique numérique plus résilient en abordant les vulnérabilités à un niveau fondamental et transfrontalier, garantissant que la sécurité d'un État membre ne compromet pas celle des autres. Cela illustre un passage d'une discrétion nationale à un cadre plus unifié et contraignant pour la protection des services critiques et de l'économie dans son ensemble.

Comment mesurez-vous concrètement l'efficacité de votre programme de sécurité ?

B. Évolution de NIS 1 à NIS 2 : Principales Nouveautés et Renforcements

La Directive NIS2 abroge et remplace la Directive NIS1 (Directive (UE) 2016/1148) à compter du 18 octobre 2024, marquant une refonte significative du cadre de cybersécurité européen. Les améliorations apportées par NIS2 sont substantielles et visent à créer un environnement numérique plus sûr et plus résilient.

L'une des différences les plus significatives réside dans l' **élargissement du champ d'application**. NIS2 couvre désormais un éventail beaucoup plus large de secteurs et d'entités, passant d'environ 19 à 35 secteurs réglementés. Cela inclut par défaut la plupart des entités de

taille moyenne et grande, ainsi que de nombreuses administrations publiques. Cette expansion vise à éliminer les "maillons faibles" causés par des organisations précédemment exemptées, renforçant ainsi la résilience globale de l'infrastructure numérique de l'UE.

Notre avis d'expert
Nos retours d'expérience montrent que les organisations qui investissent dans la lecture et l'application de référentiels méthodologiques structurés réduisent leur temps de réponse aux incidents de 40% en moyenne. La connaissance formalisée est un avantage compétitif sous-estimé.

NIS2 impose des **exigences de sécurité plus strictes et harmonisées**. La directive mandate l'adoption de mesures de gestion des risques plus rigoureuses et standardisées, basées sur une approche "tous risques". Ces mesures doivent être appropriées et proportionnées aux risques encourus, et incluent des éléments spécifiques tels que la sécurité de la chaîne d'approvisionnement, l'authentification multi-facteurs, et des communications sécurisées.

Un autre renforcement majeur concerne la **responsabilité accrue de la direction**. Les organes de direction des entités concernées sont désormais tenus personnellement responsables de la conformité aux mesures de gestion des risques de cybersécurité et de leur mise en œuvre. La directive exige également que les membres de ces organes de direction suivent des formations régulières en cybersécurité pour acquérir les connaissances et compétences nécessaires à l'évaluation des risques et des pratiques de gestion.

Les **obligations de notification d'incidents sont améliorées et précises**. NIS2 standardise et rationalise les exigences de signalement, les rendant plus précises et cohérentes. Les entités doivent notifier les autorités nationales compétentes des incidents significatifs selon un processus en plusieurs étapes avec des délais stricts : une alerte précoce dans les 24 heures, une notification d'incident dans les 72 heures, et un rapport final dans un délai d'un mois. Pour approfondir, consultez Livre Blanc Détaillé :.

Enfin, NIS2 introduit des **sanctions plus dissuasives** pour non-conformité. Les amendes financières peuvent atteindre des montants significatifs : jusqu'à 10 millions d'euros ou 2% du chiffre d'affaires annuel mondial total pour les entités essentielles (EE), et jusqu'à 7 millions d'euros ou 1.4% pour les entités importantes (EI). Des sanctions non monétaires, telles que des injonctions de conformité ou des interdictions temporaires d'exercer des fonctions de direction, peuvent également être imposées.

Le tableau suivant résume les principales distinctions entre NIS1 et NIS2 :

Caractéristique	Directive NIS 1 (2016/1148)	Directive NIS 2 (2022/2555)
Champ d'Application	Principalement les Opérateurs de Services Essentiels (OSE) dans des secteurs critiques (énergie, transport, santé, finance, eau, infrastructure numérique) et certains Fournisseurs de Services Numériques (FSN).	Élargi à un éventail beaucoup plus large de secteurs (passant de 19 à 35), incluant par défaut les entités de taille moyenne et grande dans des secteurs hautement critiques et autres secteurs critiques, ainsi que de nombreuses administrations publiques.
Exigences de Sécurité	Mesures générales de cybersécurité.	Mesures plus strictes, complètes et harmonisées, basées sur une approche "tous risques". Inclut des mesures obligatoires comme la sécurité de la chaîne d'approvisionnement, l'authentification multi-facteurs, et les communications sécurisées.
Responsabilité	Moins d'accent sur la responsabilité des dirigeants.	Responsabilité accrue et personnelle des organes de direction, avec obligation de formation en cybersécurité.
Notification d'Incidents	Exigences souvent ambiguës et incohérentes entre les États membres. Délais non uniformisés.	Processus de notification standardisé et précis en plusieurs étapes : alerte précoce (24h), notification d'incident (72h), rapport final (1 mois).
Sanctions	Variables selon les États membres, généralement moins sévères.	Plus dissuasives, avec des amendes financières significatives (jusqu'à 10 M€ ou 2% du CA mondial pour les EE, 7 M€ ou 1.4% pour les EI) et des sanctions non monétaires (interdictions temporaires pour les dirigeants).
Coopération Européenne	Mise en place du réseau des CSIRT et du Groupe de Coopération.	Renforcement de ces mécanismes et création de EU-CyCLONe pour la gestion des crises cyber à grande échelle.

C. Articulation avec d'Autres Réglementations Européennes (DORA, CRA)

NIS2 ne doit pas être perçue comme une réglementation isolée, mais plutôt comme une composante d'un ensemble plus vaste d'initiatives législatives de l'Union Européenne visant à renforcer la résilience cyber et la sécurité numérique. Cette approche réglementaire "par couches" est une caractéristique notable de la stratégie européenne.

Le **Règlement sur la Résilience Opérationnelle Numérique (DORA - Digital Operational Resilience Act)**, par exemple, se concentre spécifiquement sur le secteur financier. Il impose des exigences détaillées en matière de résilience opérationnelle numérique aux entités financières, couvrant la gestion des risques TIC, le signalement des incidents, les tests de résilience opérationnelle numérique, la gestion des risques liés aux tiers TIC, et le partage d'informations. Pour les entités financières relevant du champ d'application de DORA, ce règlement prévaut sur NIS2 en matière de cybersécurité, évitant ainsi la superposition d'obligations. Cela signifie que

les banques, les infrastructures de marchés financiers, et d'autres acteurs financiers spécifiquement couverts par DORA, suivront les règles de DORA pour leur cybersécurité plutôt que celles de NIS2, bien que les objectifs sous-jacents de résilience soient similaires.

Cas concret
L'ANSSI a publié en 2023 son guide de recommandations pour l'administration sécurisée des SI, mettant à jour les principes de Tiering et de bastionnement. Ce document de référence pour les organisations françaises rappelle que les fondamentaux de l'hygiène informatique restent les mesures les plus efficaces.

Votre stratégie de cybersécurité repose-t-elle sur un référentiel méthodologique éprouvé ?

Parallèlement, le **Cyber Resilience Act (CRA)** vise à garantir la cybersécurité des produits numériques (matériels et logiciels) tout au long de leur cycle de vie. Le CRA introduit des exigences de sécurité dès la conception (Security by Design) et tout au long de la chaîne d'approvisionnement des produits connectés. Il s'agit de s'assurer que les produits mis sur le marché européen sont intrinsèquement sécurisés, réduisant ainsi la surface d'attaque pour les utilisateurs et les organisations.

L'émergence simultanée de DORA, CRA et NIS2 révèle une stratégie européenne de régulation cyber "par couches" ou "sectorielle". Plutôt qu'une seule loi universelle, l'UE adopte une approche ciblée pour des secteurs spécifiques (finance avec DORA), des produits (CRA) et des services essentiels (NIS2). Cette spécialisation est une réponse à la nature diverse et complexe des risques cyber à travers différentes industries et domaines technologiques. Une loi générique unique pourrait ne pas être suffisamment efficace pour aborder les défis uniques de la résilience opérationnelle financière par rapport à la sécurité des produits connectés, par exemple. Cette approche vise une régulation plus précise et plus efficace. Pour les organisations, en particulier celles qui opèrent dans plusieurs secteurs ou qui sont impliquées dans le développement et la distribution de produits numériques, cela nécessite une stratégie de conformité complexe et intégrée. Il est impératif d'identifier les chevauchements, de prioriser les efforts et d'assurer la cohérence entre les différents cadres de cybersécurité. Cela implique un avenir où la cybersécurité est de plus en plus intégrée dès la conception des produits et dans les opérations sectorielles, allant au-delà d'une vision purement informatique pour englober une considération holistique du risque numérique à l'échelle de l'entreprise.

II. Périmètre d'Application de NIS 2 en France

A. Secteurs d'Activité Concernés

La Directive NIS2 élargit considérablement le champ d'application de NIS1, visant à couvrir un plus grand nombre d'entités dont la perturbation des services pourrait avoir un impact significatif sur l'économie ou la société. La directive s'applique principalement aux entités de taille moyenne et grande opérant dans des secteurs jugés d'une criticité élevée ou d'autres secteurs critiques. Pour approfondir, consultez Livre Blanc Détaillé :.

Les secteurs sont classifiés en deux catégories principales :

Secteurs de Haute Criticité (Annexe I) :
Ces secteurs sont considérés comme vitaux pour le fonctionnement de la société et de l'économie. Ils incluent :

- **Énergie :** Production, distribution et transmission d'électricité, y compris les points de recharge ; chauffage et refroidissement urbains ; production, stockage et pipelines de pétrole ; systèmes d'approvisionnement, de distribution et de transmission de gaz, ainsi que le stockage ; et l'hydrogène.
- **Transports :** Transport aérien, ferroviaire, par voie navigable et routier.
- **Banque et Infrastructures des Marchés Financiers :** Établissements de crédit, opérateurs d'infrastructures de marchés financiers (tels que les bourses et les contreparties centrales).
- **Santé :** Fournisseurs de soins de santé (hôpitaux, cliniques), fabricants de produits pharmaceutiques de base et de dispositifs médicaux critiques, et laboratoires de référence de l'UE.
- **Eau Potable et Eaux Usées :** Fournisseurs d'eau potable et gestionnaires d'eaux usées.
- **Infrastructure Numérique :** Fournisseurs de services de centres de données, de services de cloud computing, de réseaux de communications électroniques publics et de services de communications électroniques accessibles au public.
- **Services TIC Gérés :** Fournisseurs de services gérés de technologies de l'information et de la communication (B2B).
- **Espace :** Opérateurs d'infrastructures spatiales.
- **Administration Publique :** Entités de l'administration publique aux niveaux central et régional, à l'exclusion du pouvoir judiciaire, des parlements et des banques centrales, ainsi que les entités exerçant des activités dans les domaines de la sécurité nationale, de la sécurité publique, de la défense ou de l'application de la loi.

Autres Secteurs Critiques (Annexe II) :
Ces secteurs sont également importants, mais avec un niveau de criticité légèrement inférieur à l'Annexe I. Ils comprennent :

- Services Postaux et d'Expédition.
- Gestion des Déchets.
- Fabrication, Production et Distribution de Produits Chimiques.
- Production, Transformation et Distribution de Denrées Alimentaires.
- **Fabrication :** Spécifiquement les dispositifs médicaux, les produits informatiques, électroniques et optiques, certains types d'équipements électriques et de machines, les véhicules automobiles, les remorques et semi-remorques, et d'autres équipements de transport.
- **Fournisseurs Numériques :** Places de marché en ligne, moteurs de recherche en ligne et plateformes de services de réseaux sociaux.
- **Recherche :** Organisations de recherche.

B. Classification des Entités : Essentielles (EE) et Importantes (EI)

NIS2 introduit une classification des entités en deux catégories principales, les "Entités Essentielles" (EE) et les "Entités Importantes" (EI), avec des obligations et des régimes de supervision différenciés. Cette distinction est basée sur une combinaison de la criticité du secteur d'activité et de la taille de l'entité.

La directive applique principalement une **règle de seuil de taille** (size-cap rule). Cela signifie que la plupart des entités de taille moyenne et grande, qu'elles soient publiques ou privées, et qui opèrent dans les secteurs listés aux Annexes I et II, sont couvertes par la directive.

Les critères de classification sont les suivants :

- **Entités Essentielles (EE) :** Sont généralement considérées comme EE les grandes entreprises appartenant à un des secteurs de haute criticité (Annexe I) qui emploient au moins 250 personnes ou dont le chiffre d'affaires annuel excède 50 millions d'euros et le total du bilan annuel excède 43 millions d'euros.
- **Entités Importantes (EI) :** Sont généralement considérées comme EI les entités qui ne sont pas classées comme EE mais qui répondent aux critères de taille suivants :
  - Les entreprises appartenant à un des secteurs de haute criticité (Annexe I) qui emploient au moins 50 personnes et dont le chiffre d'affaires ou le bilan annuel excède 10 millions d'euros.
  - Les entreprises de taille intermédiaire ou grande appartenant à d'autres secteurs critiques (Annexe II).
  - Les entités de taille moyenne (50 à 250 employés, ou chiffre d'affaires entre 10 et 50 millions d'euros, ou bilan annuel entre 10 et 43 millions d'euros) dans les secteurs de haute criticité.

Il existe cependant des **exceptions à la règle de taille**, où certaines entités sont couvertes par la directive quelle que soit leur taille. C'est le cas, par exemple, des fournisseurs de réseaux de communications électroniques publics, des services de communications électroniques accessibles au public, des fournisseurs de services de confiance, et des fournisseurs de registres de noms de domaine de premier niveau et de services de système de noms de domaine. De plus, les États membres peuvent désigner d'autres entités comme essentielles ou importantes si elles sont le seul prestataire d'un service essentiel sur le territoire national, ou si la perturbation de leur service par une cyberattaque pourrait avoir un impact systémique. Pour approfondir, consultez Top 10 Solutions EDR/XDR.

En France, pour déterminer la taille d'une entité, les critères retenus sont un nombre d'employés supérieur ou égal à 50, ou un chiffre d'affaires ou bilan annuel supérieur ou égal à 10 millions d'euros. Cela a un impact significatif sur les **Petites et Moyennes Entreprises (PME)**, car même si elles ne sont pas directement soumises à toutes les obligations de NIS2 en tant qu'EE ou EI, elles sont souvent des maillons critiques dans la chaîne d'approvisionnement des grandes entités et devront donc se conformer aux exigences contractuelles de leurs clients.

Les **collectivités territoriales** sont également fortement impactées. Environ 15 000 entités publiques et privées seront concernées en France, dont environ 1 500 collectivités en tant qu'entités essentielles. Les communes de plus de 30 000 habitants et leurs intercommunalités

de rattachement seront notamment concernées. La Commission supérieure du numérique et des postes (CSNP) a émis des recommandations pour préciser la notion d'"incident important" et pour un accompagnement technique et financier des collectivités, suggérant une souplesse dans l'appréciation du respect des obligations jusqu'au 31 décembre 2027.

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a mis à disposition un simulateur en ligne via la plateforme "MonEspaceNIS2" pour aider les organisations à déterminer leur statut indicatif. ce simulateur fournit un résultat purement indicatif, le périmètre définitif dépendant de la transposition finale de la directive et des décrets d'application.

Le passage d'une détermination nationale discrétionnaire des opérateurs de services essentiels sous NIS1 à une classification plus harmonisée et basée sur la taille sous NIS2 représente une évolution significative. Cette harmonisation vise à apporter une plus grande clarté et prévisibilité pour les entités concernées à travers l'UE, tout en permettant aux États membres d'adapter certaines spécificités nationales. Cela réduit les divergences d'interprétation et renforce la cohérence du cadre réglementaire, facilitant ainsi la conformité transfrontalière et la résilience collective face aux cybermenaces.

C. Entités Exclues du Champ d'Application

Bien que la Directive NIS2 étende considérablement son champ d'application, certaines entités et activités spécifiques sont explicitement exclues de ses dispositions. Ces exclusions sont généralement motivées par des considérations de sécurité nationale, de souveraineté ou par la nature intrinsèque de leurs fonctions, qui sont souvent déjà régies par des cadres juridiques distincts et rigoureux.

La directive ne s'applique pas aux entités de l'administration publique qui exercent des activités dans les domaines suivants :

- Sécurité nationale
- Sécurité publique
- Défense
- Application de la loi

certaines institutions gouvernementales centrales sont également exclues, à savoir : Pour approfondir, consultez Livre Blanc Détaillé :.

- Le pouvoir judiciaire
- Les parlements
- Les banques centrales

Ces exclusions reconnaissent que ces domaines et entités sont souvent soumis à des régimes de sécurité et de confidentialité très spécifiques et potentiellement plus stricts, qui relèvent de la souveraineté nationale et ne peuvent être harmonisés de la même manière au niveau de l'UE. Par exemple, les activités liées à la défense et à la sécurité nationale sont intrinsèquement liées aux intérêts fondamentaux de l'État, justifiant des cadres réglementaires adaptés et souvent classifiés. Il est important de souligner que même si ces entités sont exclues de l'application directe de NIS2, cela ne signifie pas qu'elles sont exemptées d'obligations en matière de

cybersécurité. Elles sont généralement soumises à des réglementations nationales équivalentes ou plus exigeantes, garantissant un niveau de protection adéquat pour leurs systèmes d'information critiques.

III. Obligations Clés de la Directive NIS 2

A. Mesures de Gestion des Risques de Cybersécurité

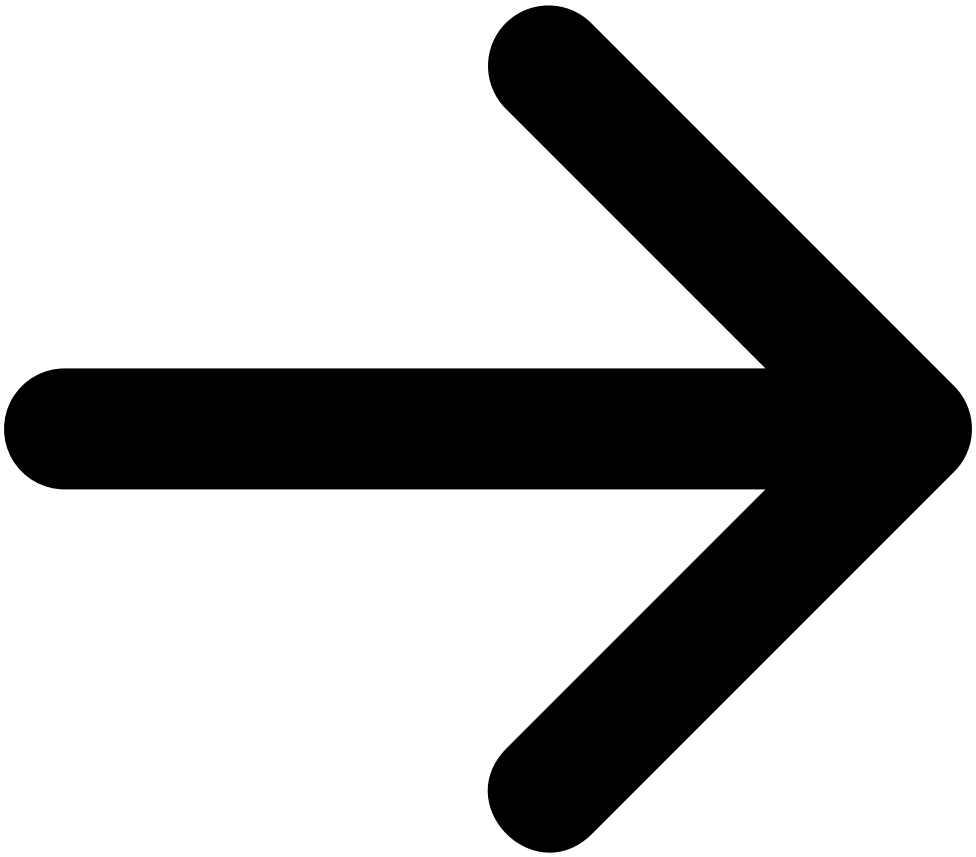
La Directive NIS2 impose un ensemble d'obligations rigoureuses aux entités essentielles (EE) et importantes (EI) afin de garantir un niveau élevé de cybersécurité et de résilience. Ces obligations couvrent la gestion des risques, la notification des incidents et la sécurité de la chaîne d'approvisionnement. NIS2 exige des entités qu'elles adoptent une approche proactive et "tous risques" pour la gestion de la cybersécurité. Cela signifie qu'elles doivent être préparées à faire face à un large éventail de menaces, des cyberattaques aux perturbations physiques, afin d'assurer une protection complète et la résilience de leurs opérations. Les mesures mises en œuvre doivent être appropriées et proportionnées aux risques identifiés, en tenant compte de l'exposition aux risques de l'entité, de sa taille, et de la probabilité et gravité des incidents, y compris leur impact sociétal et économique. La directive énumère une liste minimale de mesures techniques, opérationnelles...

Préparez votre organisation à la conformité NIS 2
Nous pouvons vous accompagner dans l'évaluation de votre maturité en cybersécurité, l'élaboration de vos plans de remédiation et la mise en place des mesures nécessaires pour être en conformité avec la directive NIS 2. Contactez-nous pour un diagnostic personnalisé.

Continuer votre lecture sur la Cybersécurité

Plongez dans un autre de nos livres blancs pour approfondir vos connaissances sur d'autres sujets de sécurité essentiels.

Voir tous nos livres blancs



Ressources open source associées :

- nis2-directive-fr — Dataset directive NIS2 (HuggingFace)
- compliance-eu-fr — Dataset conformité UE (HuggingFace)

Questions frequentes

Comment ce sujet impacte-t-il la securite des organisations ?

Ce sujet a un impact significatif sur la securite des organisations car il touche aux fondamentaux de la protection des systemes d'information. Les entreprises doivent evaluer leur exposition, déployer des mesures preventives adaptees et former leurs equipes pour faire face aux risques associes a cette problematique.

Quelles sont les bonnes pratiques recommandees par les experts ?

Pourquoi est-il important de se former sur ce sujet en 2026 ?

En 2026, la maitrise de ce sujet est devenue incontournable face a l'evolution constante des menaces et des exigences reglementaires. Les professionnels de la cybersecurite doivent maintenir leurs competences a jour pour proteger efficacement les actifs numeriques de leur organisation et repondre aux obligations de conformite.

Conclusion

Sources et références : ANSSI · CERT-FR

Outils et Ressources Conformite NIS 2

Decouvrez nos outils open source et modeles d'IA developpes pour les professionnels de la cybersecurite :

Outil / Ressource	Description	Lien
ComplianceBot	Bot d''audit automatise pour la verification de conformite reglementaire	Voir sur GitHub
ISO27001-Expert-1.5B	Expert IA ISO 27001, norme de reference pour la conformite NIS 2	Voir sur HuggingFace
RGPD-Expert-1.5B	Expert RGPD pour la conformite des donnees dans le cadre NIS 2	Voir sur HuggingFace
Compliance Assistant	Assistant interactif de conformite pour les directives europeennes	Voir sur HuggingFace
Awesome Cybersecurity Tools	Collection d''outils de securite pour la mise en conformite NIS 2	Voir sur GitHub

Tous ces outils sont disponibles en open source sur notre profil GitHub et nos modeles d'IA sur notre espace HuggingFace. N'hesitez pas a contribuer et a signaler les issues.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr