DPO FORUM
Paris 2024

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

Faire de NIS2 une opportunité pour protéger ses données personnelles de façon souveraine

Olivier MOREL
Trésorier HEXATRUST
DG Adjoint SNOWPACK
olivier.morel@snowpack.eu

DPO FORUM

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

DPO FORUM

Qui sommes-nous ?

HEXATRUST, LE GROUPEMENT DES CHAMPIONS FRANÇAIS ET EUROPÉENS DE LA CYBERSÉCURITÉ ET DU CLOUD DE CONFIANCE

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

L’association Hexatrust

Hexatrust est une association loi 1901 née en 2013.

Elle regroupe et fédère les champions français et européens de la **cybersécurité**, du **cloud de confiance** & du **digital workplace**.

L’association représente ses adhérents **auprès des pouvoirs publics** et mène de nombreuses actions de **mise en valeur** de ses membres et de la filière. A ce titre, elle est **au cœur de l’écosystème cyber**, partenaire des **grands évènements cyber** en France et en Europe et participante aux travaux des Comités Stratégiques de Filière.

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

Quelques chiffres …

123
sociétés adhérentes
au 1er janvier 2024

2,3
milliards d'€
de CA cumulés

1000+
Inscrits aux
Universités d'été 2023

+30%
de croissance
en 2023

Nos adhérents sont des start-up, des PME & ETI de la cybersécurité et de la confiance numérique : éditeurs de solutions de cybersécurité, fournisseurs de Cloud de confiance (SaaS, PaaS, IaaS), Entreprises de Services du Numérique, Cabinets de conseil, utilisateurs, avocats et DPO, courtiers d'assurance, établissements de financement…

30% de leur CA est réalisé à l'export, 30 % est réinvesti en innovation, en croissance constante chaque année.

DPO FORUM

L'union fait la force

Défendre

Accompagner les évolutions réglementaires et défendre les intérêts de nos adhérents

Représenter

Porte-parole de nos membres au sein des instances représentatives de la filière et animateur d'un écosystème tourné vers le développement entrepreneurial

Promouvoir

Valoriser la filière en France et à l'international et faire connaître au plus grand nombre les enjeux de la cybersécurité et du cloud de confiance

Unis pour construire ensemble une filière engagée pour un monde numérique plus sûr, résilient et protecteur des données.

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

#Défendre

International

Labels

FRANCE CYBER SECURITY

CYBERSECURITY MADE IN EUROPE™

Solutions et Services

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

#Représenter

Auprès des pouvoirs publics

Auprès de la filière

CSF Industries de sécurité
CSF Numérique de confiance

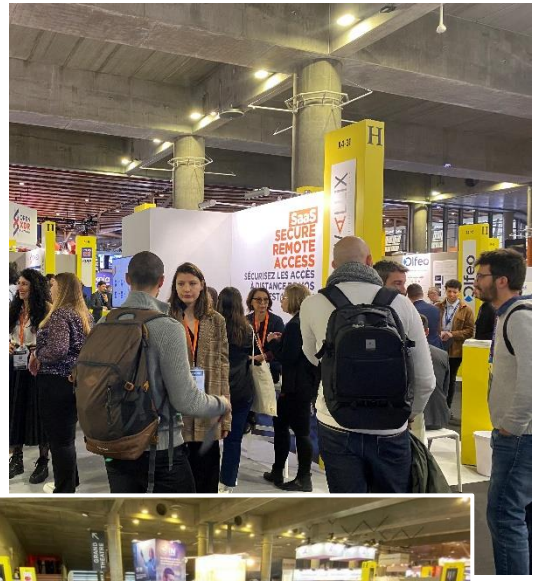
Auprès du monde économique

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

#Promouvoir

Universités d'été HEXATRUST

RENDEZ-VOUS
LE 5 SEPTEMBRE 2024
À STATION F



Forum InCyber EU
Forum InCyber NA
Les Assises
CoTer numérique
Sant'Expo
CyberCamp Santé
Cybershow Paris

… CyberSec, tour de France CAIH, tour de France UGAP, European Cyber Week, Eurosatory, SIT Africa …

Nos adhérents

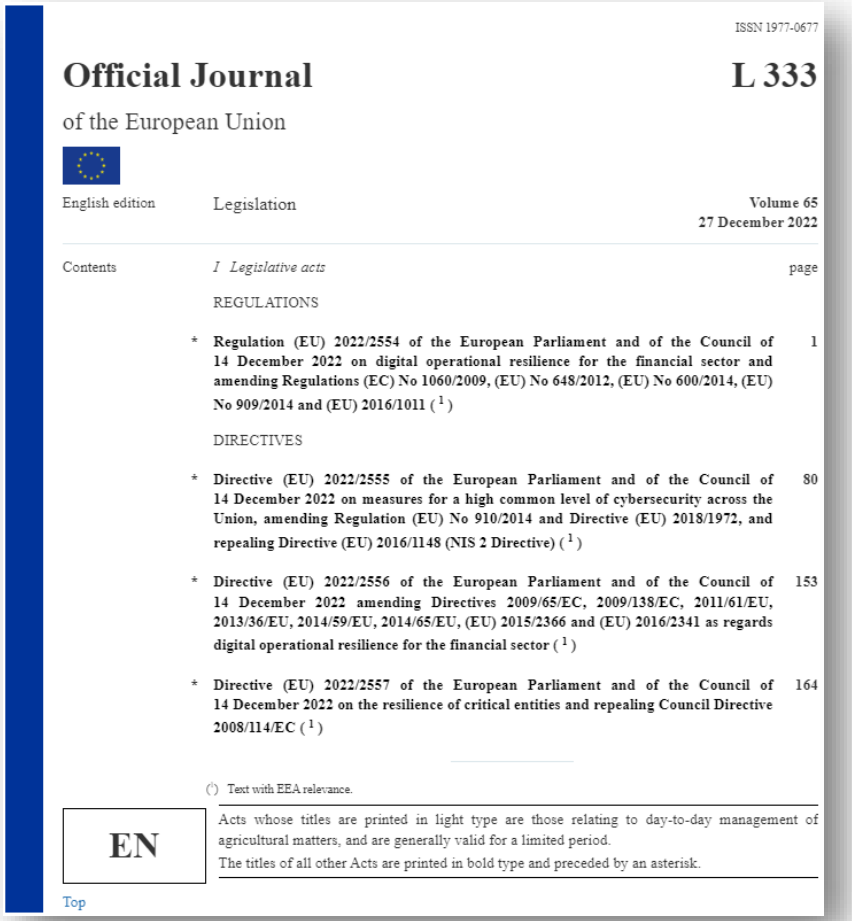
DPO FORUM

(rappels sur) la directive NIS2

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

Chronologie …

- **2013** : LPM (*Loi de programmation militaire*)
- **Avril 2016** : RGPD *(Règlement Général sur la Protection des Données)*
- **Juillet 2016** : NIS *(Network Information systems Security)*
  - Transposée en droit français en 2018
  - ~300 entités désignée OSE (*Opérateurs de Services Essentiels*)
- **Décembre 2022** : NIS2
  - + directive REC (*Résilience des Entités Critiques*)
    + réglementation DORA (*Digital operational resilience act*)
- **18 Octobre 2024** : Transposition en droit interne
- Liens :
  - https://cyber.gouv.fr/la-directive-nis-2
  - https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv%3AOJ.L_.2022.333.01.0080.01.FRA&toc=OJ%3AL%3A2022%3A333%3ATOC



ISSN 1977-0677

Official Journal **L 333**

of the European Union

English edition Legislation Volume 65
27 December 2022

Contents *I Legislative acts* page

REGULATIONS

([1]) Text with EEA relevance.

EN

Acts whose titles are printed in light type are those relating to day-to-day management of agricultural matters, and are generally valid for a limited period.
The titles of all other Acts are printed in bold type and preceded by an asterisk.

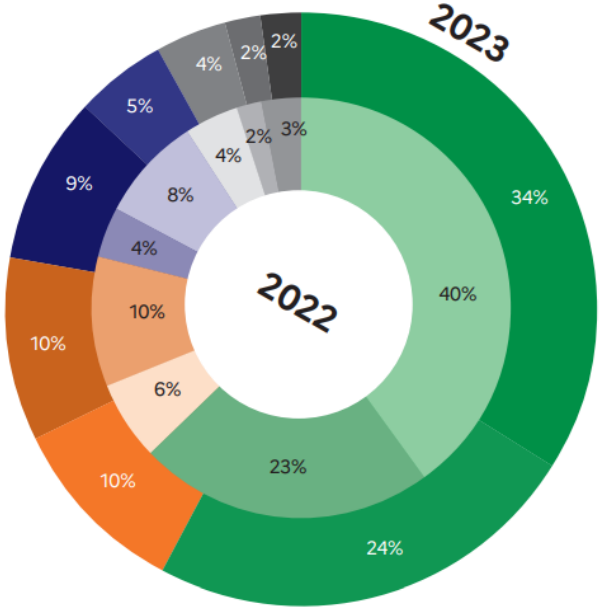
Top

Pourquoi une directive NIS… 2 ?

- Hétérogénéité importante entre les états membres de l'UE

- Evolution de la menace
  - Nouvelles cibles : PME, ETI, collectivités territoriales
  - Conséquences dramatiques des cyber-attaques
  - Chaîne d'approvisionnement

- Et aussi :
  - Ouverture du SI / Cloud,
  - Explosions du nombre de dépendances (et vulnérabilités) logicielles,
  - IA…



→ Répartition des victimes d'attaque par rançongiciel

TPE/PME/ETI
Collectivité territoriale/locale
Entreprise stratégique
Établissement de santé
Association
Établissement d'enseignement s
EPA, EPIC
Ministère
Autre

ANSSI : Panorama de la cybermenace 2023

CVE	ÉDITEUR	CVSS SCORE [20]	RÉFÉRENCE CERT-FR
CVE-2021-21974	VMWARE	8.8	CERTFR-2023-ALE-015 CERTFR-2021-AVI-145
CVE-2023-20198	CISCO	10.0	CERTFR-2023-ALE-011 CERTFR-2023-AVI-0878
CVE-2023-3519	CITRIX	9.8	CERTFR-2023-ALE-008 CERTFR-2023-AVI-0568
CVE-2023-22518	ATLASSIAN	9.8	CERTFR-2023-AVI-0899 CERTFR-2023-ACT-048
CVE-2023-34362	PROGRESS SOFTWARE	9.8	CERTFR-2023-ALE-005

Top 5 des vulnérabilités les plus exploitées en 2023

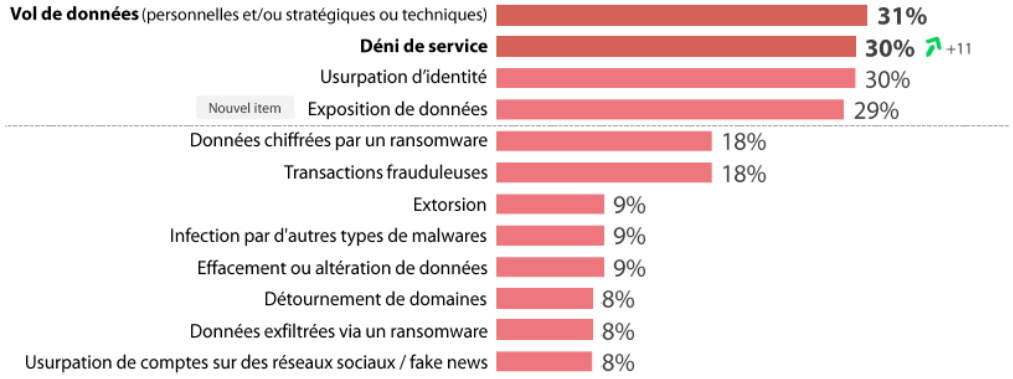
Quelques chiffres …

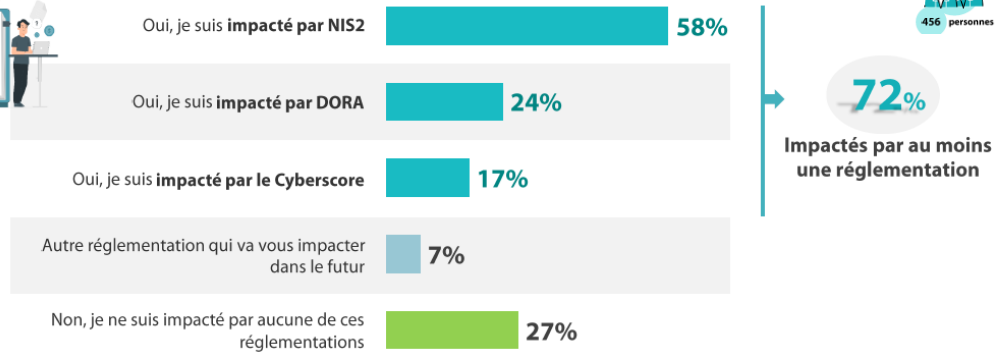
9ème édition du baromètre annuel du CESIN (janvier 2024)

"opinionway pour CESIN

225 personnes

49% des entreprises ont subi au moins une cyberattaque en 2023





456 personnes

72% Impactés par au moins une réglementation

"Les risques sur le contrôle des sous-traitants et des accès par les administrateurs restent les plus importants, les défauts de cloisonnement entre les différents clients de l'hébergeur sont de plus en plus problématiques, heureusement le niveau d'expertise augmente

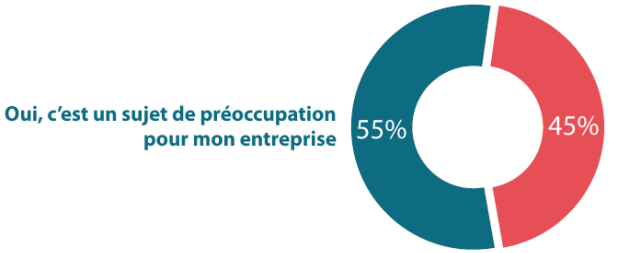
456 personnes

Q21. Selon vous, les facteurs suivants représentent-ils un risque faible, modéré ou fort en ce qui concerne l'utilisation du Cloud ?
Base : ensemble

Rappel classement 2022		% Un risque fort	
1	1	48%	**Non maîtrise de la chaîne de sous-traitance de l'hébergeur**
2	2	43%	**Difficulté de contrôler les accès par des administrateurs de l'hébergeur**
		40%	Mauvaise visibilité de l'inventaire des ressources qu'il y a dans le cloud
4		39%	Stockage des données en France/Europe mais assuré et/ou opéré par des prestataires étrangers où la loi du pays d'origine s'applique également
		37%	Stockage des données dans des datacenters à l'étranger, hors du droit français
+10		37%	Défaut de cloisonnement entre les différents clients de l'hébergeur
5		36%	Difficulté de mener des audits (test d'intrusion, contrôle des configurations, visite sur site)
Item modifié		36%	Non-maîtrise des paramètres de sécurité / chiffrement faible de la part de l'hébergeur (l'hébergeur gère les clés de déchiffrement)
-9	3	34%	Expertise encore trop rare, attendue de la part des architectes et des administrateurs
		33%	Indisponibilité des données / de l'application due à une attaque de l'hébergeur

Souveraineté et Cloud de Confiance

456 personnes



HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

NIS → NIS2

LES ENTITÉS ESSENTIELLES ET IMPORTANTES

SCHÉMATISATION SIMPLIFIÉE DE LA RÈGLE DE BASE

TAILLE ENTITE	NOMBRE D'EMPLOYÉS	CHIFFRE D'AFFAIRES (MILLIONS D'EUROS)	BILAN ANNUEL (MILLIONS D'EUROS)	SECTEURS HAUTEMENT CRITIQUES	AUTRES SECTEURS CRITIQUES
Intermédiaire et grande	X ≥ 250	Y ≥ 50	Z ≥ 43	Entites essentielles	Entites importantes
Moyenne	50 ≥ X ≥ 250	10 ≥ Y > 50	10 ≥ Z > 43	Entites importantes	Entites importantes
Micro et petite	X<50	Y <10	Z<10	Non concernées	Non concernées

Les secteurs concernés

Un régime de sanctions sévère

Entité essentielle :
Amende administrative
10 000 000 € ou égale à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent

Entité importante :
Amende administrative
7 000 000 € ou égale à 1,4 % du chiffre d'affaires annuel mondial total de l'exercice précédent

Responsabilité du dirigeant engagée en cas de manquement :
Pénale ou civile*
**en fonction de la transposition de la directive en droit national*

Obligations pour les entités régulées

- Obligation de **notification** et **d'information** de tout incident de cybersécurité à l'autorité nationale compétente *(à l'instar du RGPD et de la notification des violations de données à la Cnil)*
  - *A noter :*

Article 35

Infractions donnant lieu à une violation de données à caractère personnel

- **Responsabiliser** les directions faces aux enjeux cyber

- **Mesures de sécurité** « appropriées et proportionnées » à prendre par les entités pour gérer les risques :
  - Techniques
  - Opérationnelles
  - Organisationnelles

Article 21

Mesures de gestion des risques en matière de cybersécurité

1. Les États membres veillent à ce que les entités essentielles et importantes prennent les mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information que ces entités utilisent dans le cadre de leurs activités ou de la fourniture de leurs services, ainsi que pour éliminer ou réduire les conséquences que les incidents ont sur les destinataires de leurs services et sur d'autres services.

Mesures de sécurité (art. 21)

2. 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 **cyberhygiène** 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.

Mais concrètement ?

DPO FORUM

Réponse Hexatrust

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

DPO FORUM

FRANCE RELANCE

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

DPO FORUM

L’effort collectif sans précédent occasionné par NIS2 doit provoquer un changement de paradigme face à la menace cyber. La France et les autres États membres de l’Union européenne s’engagent aujourd’hui dans une plus intense coopération pour mettre au ban les groupes cybercriminels, qui ne connaissent pas de frontières, et renforcer notre souveraineté numérique européenne. Dans le même temps, nous comptons sur l’écosystème cyber français pour répondre présent

Marina Ferrari
Secrétaire d’État chargée du Numérique

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

DPO FORUM

Réunis au sein du groupement Hexatrust, les acteurs français de la cyber souhaitent être des partenaires incontournables et de confiance au service de l'économie nationale, et du renforcement de sa sécurité numérique. Ils sont mobilisés pour accompagner nos entreprises, nos organisations, en leur offrant des solutions adaptées à leur besoin, de manière coordonnée, tout en leur permettant de répondre facilement aux nouvelles obligations mises en place par la NIS2.

Jean-Noël de Galzain
Président d'Hexatrust,
Vice-Président du CSF « Industries de sécurité »

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

La communauté se mobilise …

David Lisnard
AMF

Jean-Paul Bonnet
CDSE

Mylène Jarossay
CESIN

Henri d'Agrain
CIGREF

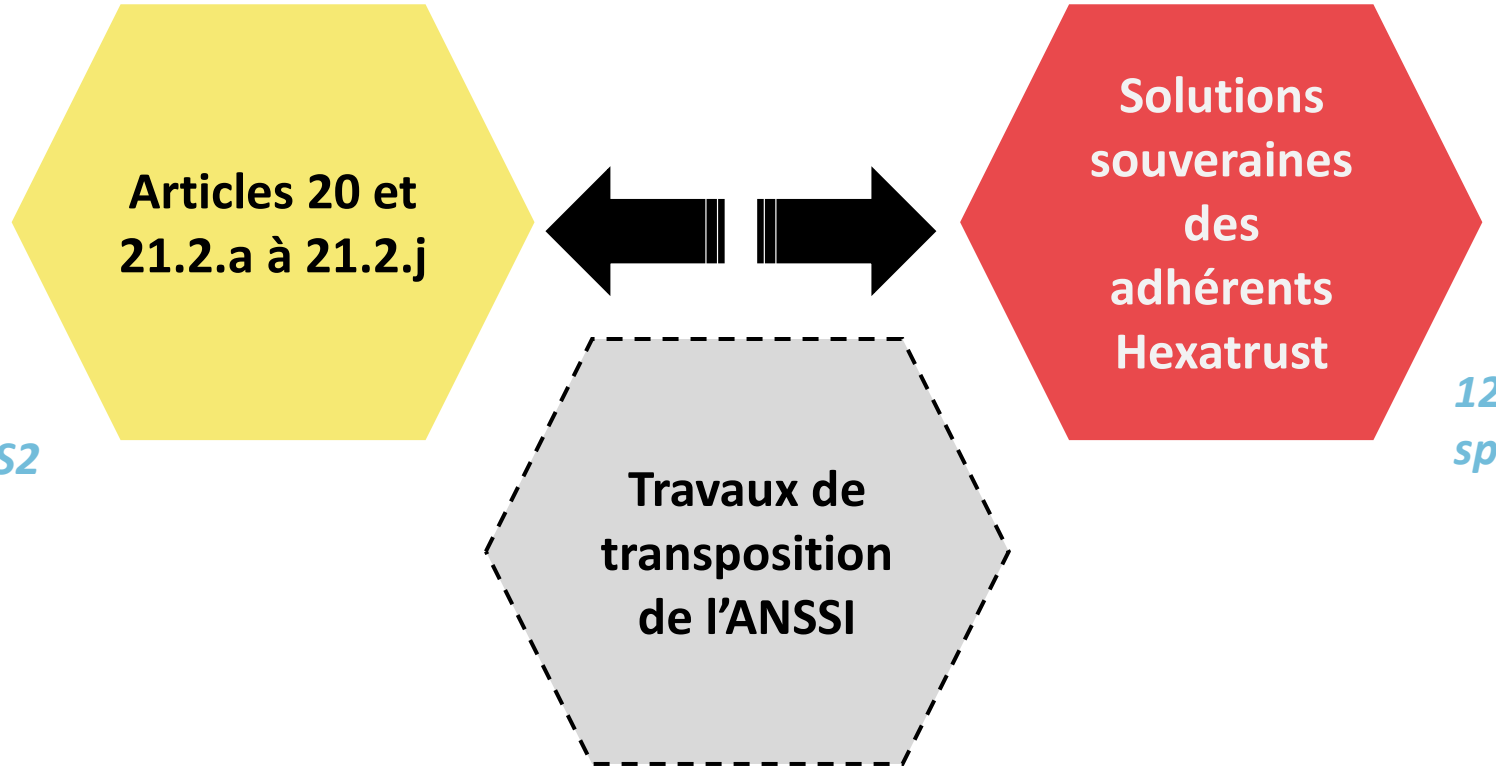
Loïc Guézo
CLUSIF

Antoine Trillard
COTER Numérique

Claire Laurent
GIFEN

Eric Freyssinet
OSSIR

Travaux réalisés



12 entrées du référentiel NIS2

123 sociétés spécialisées

Mesures de sécurité

Exemple

Article 21.2.h « des politiques et des procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement »

Il s'agit de sécuriser l'architecture de ses systèmes d'information, notamment eu égard aux **accès distants**. Mais cette disposition peut être également mise en lien avec les sujets de PSSI pour intégrer dans ces politiques et procédures la micro-segmentation du système d'information et le recours à une architecture Zero-Trust.

Micro-segmentation & ZTNA, firewall, gateway, IPS, WAF.. / sécu interconnexions infra & app, filtrage communications (DNS, etc.) / gestion des accès M2M

Objectif de sécurité 2. L'entité dispose d'un cadre de gouvernance de la sécurité numérique
Objectif de sécurité 9. L'entité sécurise l'architecture de ses systèmes d'information réglementés
Objectif de sécurité 10. L'entité sécurise les accès distants à ses systèmes d'information réglementés

DPO FORUM

Comment les adhérents d'Hexatrust peuvent répondre à vos besoins de mise en conformité à NIS2

Le tableau qui suit comporte :

- selon les colonnes verticales, les dispositions des articles 20 et 21 de NIS2 sur lesquelles nous nous sommes appuyé pour créer ce référentiel ;
- selon les lignes horizontales, les sociétés offrant des solutions et/ou services en réponse aux dispositions associées.

	Art. 20	Art. 21.2	Art. 21.2.a	Art. 21.2.b	Art. 21.2.c	Art. 21.2.d	Art. 21.2.e	Art. 21.2.f	Art. 21.2.g	Art. 21.2.h	Art. 21.2.i	Art. 21.2.j
6CURE				x			x	x		x		
AISI	x		x	x	x	x	x	x	x		x	
ALGOSECURE	x		x	x	x	x	x	x	x	x	x	x
ALTOSPAM					x		x		x	x	x	
ANTEMETA					x		x					
ARCAD SOFTWARE							x	x				
ASTRAN					x					x		
ATEMPO		x			x			x				x
AUCAE				x	x				x			
AVANT DE CLIQUER									x			
AXIANS	x		x	x	x	x	x	x	x	x	x	
BELLEDONNE COMMUNICATION							x					x
BLUEMIND					x							x
BOARD OF CYBER			x			x	x				x	
BONJOURCYBER	x		x	x	x	x	x	x	x		x	
BRAIN NETWORKS	x		x	x			x	x	x		x	
BRAIN SECURITY									x			
CONSCIO TECHNOLOGIES									x			
CONTINUS.IO						x	x	x				
CROWDSEC				x			x				x	
CRYPTONEXT SECURITY							x			x		x
CUSTOCY				x			x					
CYBER-DETECT			x	x		x						
CYBERIUM							x			x		
CYBERVADIS						x						
CYBERWATCH			x				x					
CYBERXPERT	x		x	x	x		x	x	x	x		
DASTRA												
DEFANTS				x				x				

	Art. 20	Art. 21.2	Art. 21.2.a	Art. 21.2.b	Art. 21.2.c	Art. 21.2.d	Art. 21.2.e	Art. 21.2.f	Art. 21.2.g	Art. 21.2.h	Art. 21.2.i	Art. 21.2.j
DELETEC	x		x	x	x		x	x	x	x	x	
DEVENSYS CYBERSECURITY	x		x	x			x	x	x			
DIGITALBERRY	x		x	x	x	x	x	x		x	x	x
DOCAPOSTE	x		x	x	x		x	x		x	x	x
EBRC	x	x	x	x	x	x	x	x	x		x	
EGERIE	x		x					x	x			
EQUISIGN					x					x	x	x
ERCOM					x							x
EVERTRUST SAS			x				x				x	x
EXCELSIOR SAFETY			x		x		x		x		x	
EXIPTEL SAS			x	x	x		x					
EXO PLATFORM												x
EY FRANCE	x		x	x	x	x	x	x	x	x	x	x
FAIRTRUST	x						x				x	x
FILIGRAN	x		x	x				x				
GATEWATCHER			x	x	x	x	x				x	
GLIMPS				x			x				x	
HARFANGLAB				x			x				x	
HIASECURE	x		x				x				x	x
HOLISEUM			x					x		x		
ILEX INTERNATIONAL							x				x	x
INQUEST	x		x	x	x			x	x			
INSPEERE					x							
ISE SYSTEMS	x		x	x		x	x	x	x		x	
ITRUST - GROUPE ILIAD				x	x		x				x	
JALIOS			x			x			x		x	x
JAMESPOT												x
LAGERTHA										x		x
LEVIIA					x							
LOGIN SECURITE	x	x	x	x	x	x	x	x	x	x	x	x
MAILINBLACK							x		x	x	x	
MAKE IT SAFE	x		x	x		x	x	x				
MATHIAS AVOCATS									x			
MEROX	x		x				x		x			
METSYS	x		x	x	x	x	x	x	x		x	x
MINDFLOW					x		x				x	
MOABI SOLUTIONS						x		x		x		
N-CYP				x	x	x	x					
NAMESHIELD	x		x				x	x			x	
NEOTECH ASSURANCES	x								x			
NEOTRUST	x		x	x	x	x	x	x	x		x	
NEOWAVE		x									x	x
NETEXPLORER			x	x	x						x	
NUMSPOT					x		x			x	x	x

	Art. 20	Art. 21.2	Art. 21.2.a	Art. 21.2.b	Art. 21.2.c	Art. 21.2.d	Art. 21.2.e	Art. 21.2.f	Art. 21.2.g	Art. 21.2.h	Art. 21.2.i	Art. 21.2.j
OLFEO							x		x		x	
OLIVIER WEBER AVOCAT												
OLVID					x					x		x
OODRIVE	x		x	x	x		x	x	x	x	x	x
OUTSCALE - DASSAULT SYSTEMS					x				x	x	x	
OVERSOC			x			x	x	x				
P4S										x	x	
PARSEC							x			x		x
PATROWL			x			x	x	x			x	
PRIM'X							x			x		
PRIVATE DISCUSS												x
PRIZM	x		x				x				x	
PROVENRUN						x	x					
QONTROL	x		x		x		x	x			x	
RESCO COURTAGE	x		x	x								
RETARUS							x					
REVERSENSE							x				x	
RYDER & DAVIS												
SCALAIR	x		x	x	x	x	x	x		x	x	
SCALITY					x							
SECLAB					x		x				x	x
SEELA									x			
SEKOIA.IO				x			x				x	
SMART GLOBAL GOVERNANCE	x		x	x	x	x		x	x			
SNOWPACK							x			x	x	
SOSAFE	x		x						x			
SURICATE							x				x	
SYNETIS	x	x	x	x	x	x	x	x	x		x	x
TENACY	x		x			x	x	x				
TERSEDIA	x		x	x	x	x	x	x	x	x	x	
THEGREENBOW						x	x			x		
TIXEO					x							x
TRANQUIL IT							x				x	
TRUSTBUILDER (INWEBO)											x	x
TRUSTINSOFT							x					
TYREX (EX. KUB)							x		x			
UBIKA							x		x			
UGLOO					x							
UNCOVERY											x	
VADE				x	x		x		x		x	
WALLIX							x				x	x
WHALLER					x							x
YESWEHACK							x	x				
YOGOSHA								x				

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

sekoia

Informations contact

Freddy Milesi | contact@sekoia.io | https://sekoia.io
54, rue des Petites écuries 75010 Paris

Description et produits

Sekoia.io est la cybertech européenne leader des solutions de détection et de réponse étendues s'appuyant sur le renseignement d'intérêt cyber (Cyber Threat Intelligence).

- **Sekoia Defend (SIEM Next-Gen)** est une plateforme SOC de détection et réponse étendue (XDR) disponible en mode SaaS, et alimentée par du renseignement cyber exclusif. Anticipation des attaques, automatisation, nombreuses intégrations et règles de détection vérifiées simplifient la protection des environnements hybrides.
- **Sekoia Intelligence (CTI)** offre une connaissance approfondie des menaces. La normalisation des flux de renseignements facilite la compréhension des attaques, intrusions et actes malveillants. Le renseignement exclusif produit est contextualisé et actionnable, bénéficiant aux équipes stratégiques et opérationnelles.

Référentiel NIS 2

Art. 21.2.b : Gestion des incidents

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

snowpack

Informations contact

MOREL Olivier | olivier.morel@snowpack.eu | +33 6 99 09 13 21
https://snowpack.eu/fr/ | Centre d'intégration NANO-INNOV,
2 Boulevard Thomas Gobert, 91120 Palaiseau

Description et produits

Snowpack est un spin-off du CEA, créée en 2021, lauréate I-lab 2022 et DeepNum20, soutenue par la stratégie d'accélération cyber.
Snowpack fournit **la technologie VIPN (Virtual & Invisible Private Network)** — très innovante et brevetée — qui permet de protéger les utilisateurs, données, composants du système d'information et services web exposés sur Internet en les rendant INVISIBLES des hackers.
Avec Snowpack les attaquants NE VOUS VOIENT PAS, ainsi ILS NE VOUS ATTAQUENT PAS !
VIPN prémunit contre de nombreuses attaques réseaux, telles que la surveillance et l'interception des communications, le scan externe du système d'information, et l'exploitation des vulnérabilités des composants et services exposés sur Internet. **Elle réduit considérablement la surface d'attaque externe des organisations,** en la rendant invisible, et élimine tout besoin de confiance dans l'infrastructure.

Référentiel NIS 2

Art. 21.2.e : Sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information

Art. 21.2.h : Politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement

Art. 21.2.i : Sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs

Smart Global Governance

Informations contact

Pascal Petitjean | pascal.petitjean@smartglobal.com
04 12 39 25 20 | www.smartglobalgovernance.com
300 rue du Vallon, "Les Vaisseaux" 06560 Valbonne

Description et produits

Smart Global Governance est l'éditeur de la plateforme Smart GRC, solution de gestion des risques et conformité utilisée par plus de 300 utilisateurs dans 100 pays.
Disponible en SaaS ou on premise, Smart GRC offre aux CISO et à leurs équipes **une solution spécialisée de gestion des risques et conformité.**

- Cartographie des risques cyber • Identification et priorisation des risques • Gestion des risques cyber • Evaluation et suivi des risques • Gestion des Incidents de sécurité • Gestion des conformités • Plus de 45 standards interconnectés (AI ACT, DORA, NIS 2, ISO 27001, GDPR) • Gestion des risques Tiers • Audit et contrôle • Plan de continuité d'activité • Data Discovery

Smart GRC est ainsi une suite de solutions spécialisées formant une plateforme globale et centralisée de gouvernance, risque et conformité pour les entreprises.

- Data & Privacy • Ethics et transparency • Legal • ESG • Health and Safety • Quality • IA Intégrée « Smart Colleague »

Référentiel NIS 2

Art. 20 : Gouvernance de la gestion des risques en matière de cybersécurité

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.b : Gestion des incidents

Art. 21.2.c : Continuité des activités

Art. 21.2.d : Sécurité de la chaîne d'approvisionnement

Art. 21.2.f : Politiques et procédures d'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité

Art. 21.2.g : Cyberhygiène et formation à la cybersécurité

sosafe

Informations contact

Yan Richard | yan.richard@sosafe.de | www.sosafe.fr
23-25 avenue MacMahon, 75017, Paris — France

Description et produits

SoSafe est **la plateforme de sensibilisation à la cybersécurité et à la gestion des risques cyber axées sur l'humain.** Notre plateforme automatisée et sans effort, modifie les comportements de vos collaborateurs pour vous sécuriser via des modules d'e-learning et des simulations de cyberattaques.
Alimentée par **les sciences du comportement** et **des algorithmes intelligents,** SoSafe permet aux sociétés de développer une culture de la cybersécurité et de transformer leurs employés en alliés contre les menaces de sécurité.

- Formation personnalisée SoSafe pour changer rapidement les comportements.
- Modules de micro-apprentissage interactifs et ludiques sur la cybersécurité.
- Simulations de phishing personnalisées.
- Tableau de bord pour mesurer votre niveau de sécurité.
- Un chatbot interactif pour alerter en cas d'urgence.

Référentiel NIS 2

Art. 20 : Gouvernance de la gestion des risques en matière de cybersécurité

Art. 21.2.a : Politiques d'analyse des risques et de la sécurité des systèmes d'information

Art. 21.2.g : Cyberhygiène et formation à la cybersécurité

Où se procurer le catalogue NIS2 Hexatrust ?

https://www.hexatrust.com/

Le mot de la fin…

PIXELS · CYBERCRIMINALITÉ

Cyberattaque de France Travail : les données de 43 millions de personnes « ont potentiellement été exfiltrées »

Les personnes concernées sont celles qui sont « actuellement inscrites » ou « précédemment inscrites au cours des 20 dernières années » à l'ex-Pôle emploi. Une enquête a été ouverte.

Par Pixels (avec AFP)

Publié le 13 mars 2024 à 18h27, modifié le 14 mars 2024 à 10h03 · Lecture 1 min.

Cyberattaque des mutuelles Viamedis et Almerys : une enquête ouverte sur le piratage des données de 33 millions de Français

Ce vol d'informations confidentielles est considéré comme l'un des plus massifs jamais enregistrés en France.

franceinfo avec AFP
France Télévisions

Publié le 09/02/2024 21:26

Temps de lecture : 1 min

- Jusqu'à présent, la protection des données à caractère personnel était l'affaire du DPO. Mais avec la directive NIS 2, les entreprises vont devoir lier cette protection avec les concepts de cybersécurité.
- Certes DSI/RSSI et DPO collaborent déjà, mais les prochaines années vont voir se renforcer ce travail conjoint afin de contrer un marché de la vente de données toujours plus grandissant.

DPO FORUM

Paris 2024

MERCI !

Hexatrust
Campus Cyber
5-7 Rue Bellini,
92800 Puteaux

contact@hexatrust.com