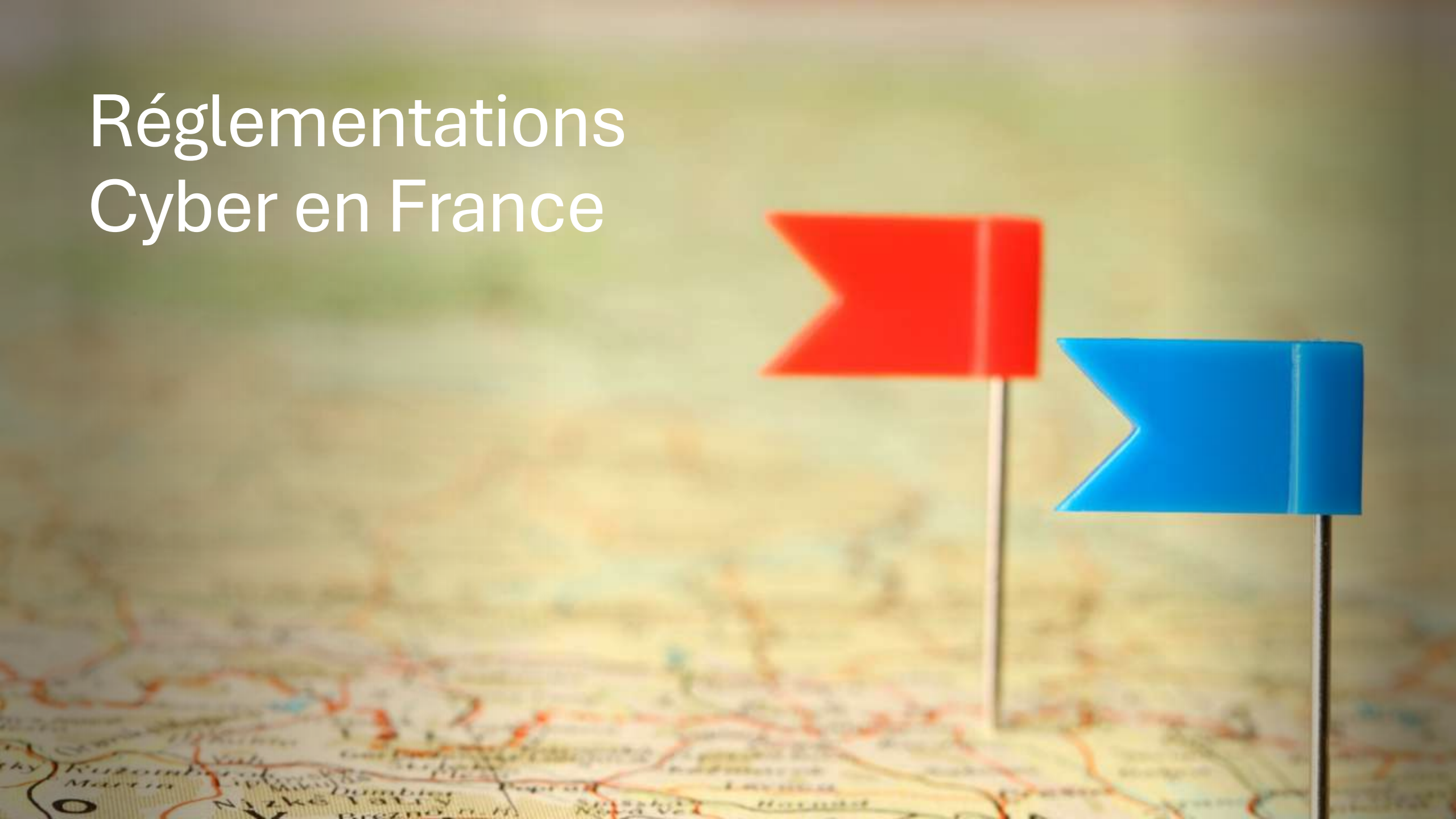
Réglementations Cyber en France



Protection des Données Personnelles et Numériques

Loi pour une République Numérique

Instructions et Décrets Interministériels

Instructions 910, 2100, 2102

Protection et Certification des Services Cloud

SECNUMCLOUD

Réglementations Cyber dans l'Union Européenne

Protection des Données Personnelles et Numériques

RGPD

Protection et Certification des Services Cloud

EUCC

Gestion des Crises et Coopération Internationale

CyCLONe

Sécurité des Infrastructures Critiques

Cyber Resilience Act

Sécurité des Infrastructures Critiques

DORA

Sécurité des Infrastructures Critiques

NIS

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

MonEspaceNIS2 BÊTA

Directive NIS 2 : Renforcer la Cybersécurité en Europe

Comprendre et Appliquer la Nouvelle Réglementation

aftec formation

Raisons de la Réglementation NIS

Contexte :

Augmentation des cyber-attaques

Importance des infrastructures critiques

Besoin de coopération internationale

Objectifs :

Renforcer la sécurité

Harmoniser les pratiques

Augmenter la résilience des systèmes

Organisation privée victime

Organisation public victime

CHIFFRES CLÉS 2023

278 770
atteintes numériques enregistrées en 2023

+40% d'atteintes numériques en 5 ans

59%
d'atteintes aux biens

34,5%
d'atteintes aux personnes

6%
d'atteintes aux institutions et à l'ordre public

0,5%
d'atteintes aux législations et règlementations spécifiques numériques

17 700
atteintes aux systèmes d'information en 2023

+28% de saisines pour des attaques par rançongiciel

THESEE

104 439 plaintes ou signalements relatifs aux escroqueries sur internet enregistrés sur la plateforme Thésée

PHAROS

211 543 signalements de contenus illicites reçus par la plateforme Pharos

PERCEV@L

259 094 signalements d'usages frauduleux de cartes bancaires répertoriés par la plateforme Perceval

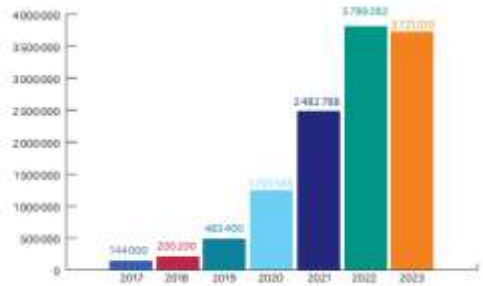
50% des victimes d'une atteinte numérique à la personne sont des femmes âgées de 18 à 44 ans

47 000 mis en cause pour des atteintes numériques

NB : Les chiffres présentés ici proviennent de données établies par le Service statistique ministériel de la sécurité intérieure, complétées par d'autres sources institutionnelles : Office Anti-Cybercriminalité de la police nationale, Unité Nationale Cyber de la gendarmerie nationale, section J3 du parquet

FRÉQUENTATION DE LA PLATEFORME CYBERMALVEILLANCE.GOUV.FR

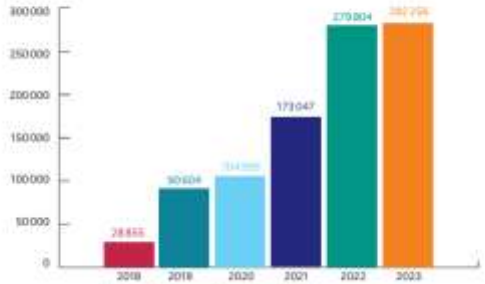
Avec 3,7 millions de visiteurs en 2023, la fréquentation de la plateforme Cybermalveillance.gouv.fr se stabilise à un niveau élevé.



Fréquentation annuelle de la plateforme Cybermalveillance.gouv.fr

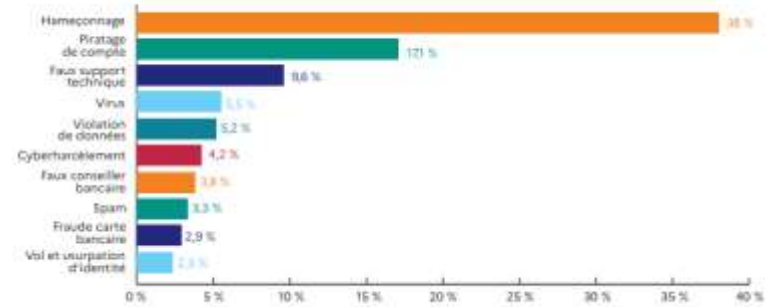
LES CHIFFRES 2023 DE LA CYBERMALVEILLANCE

L'analyse des plus de 280000 demandes d'assistance en ligne sur la plateforme Cybermalveillance.gouv.fr donne une vision des différentes formes de cybermalveillance rencontrées par les publics du dispositif.



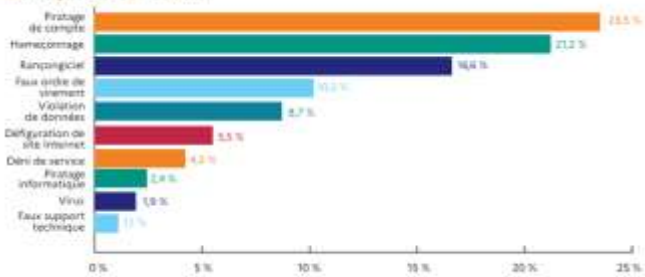
Évolution des recherches d'assistance

• Particuliers



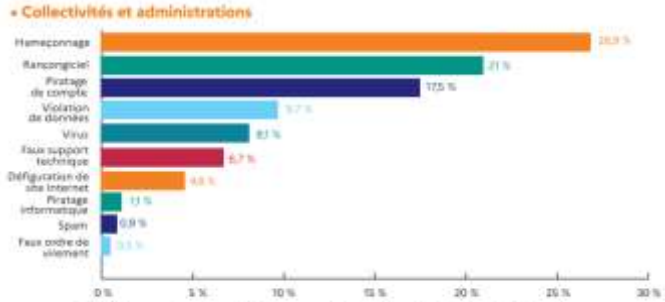
Principales recherches d'assistance pour les particuliers

• Entreprises et associations

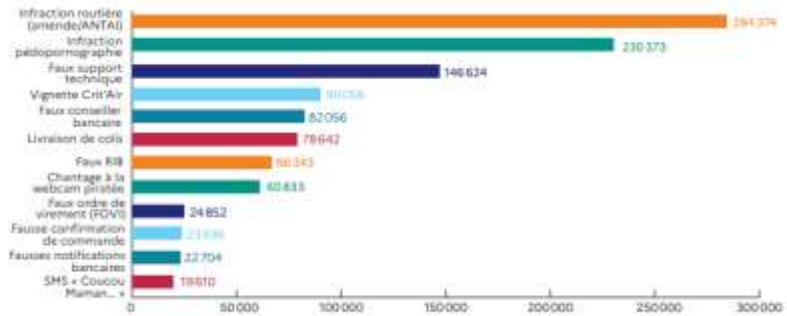


Principales recherches d'assistance pour les entreprises et les associations

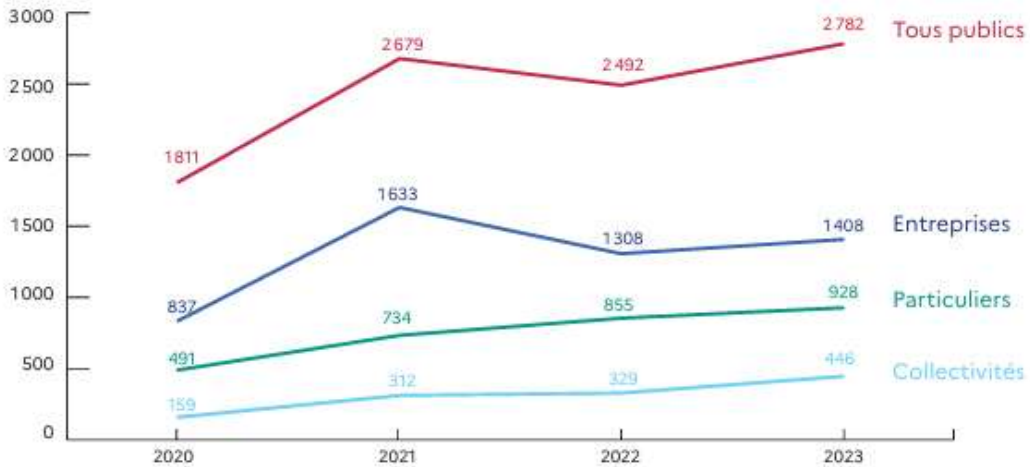
• Collectivités et administrations



Principales recherches d'assistance pour les collectivités et les administrations

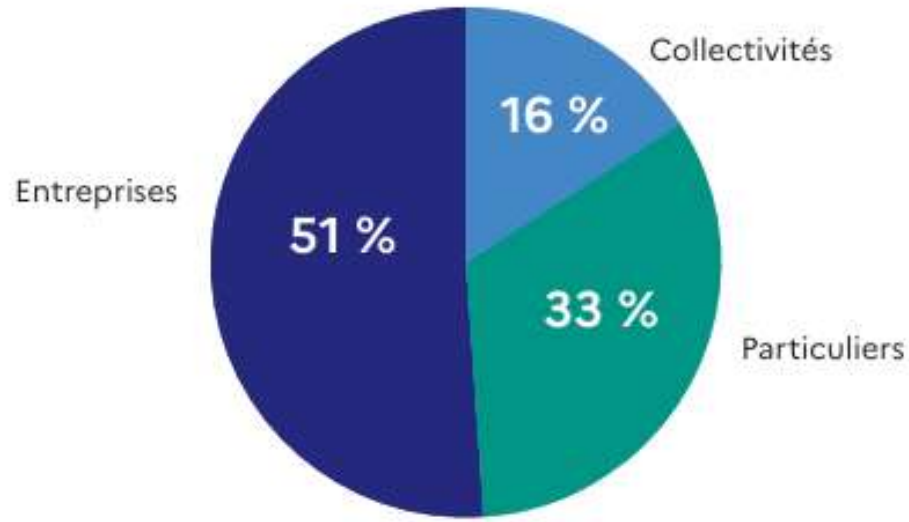


Hameçonnages les plus fréquents en 2023 (nombre de consultations)



Évolution des demandes d'assistance pour des attaques par rançongiciels

	2020	2021	2022	2023	Variation n-1
Tous publics	1 811	2 679	2 492	2 782	+12 %
Particuliers	491	734	855	928	+9 %
Entreprises	837	1 633	1 308	1 408	+8 %
Collectivités	159	312	329	446	+36 %



Impact des Cyberattaques sur les infrastructures critique

- Perturbation des services essentiels
- Risques économiques
- Sécurité publique
- Stabilité politique

Élaboration de la Réglementation

NIS

Financement de la Réglementation

- Fonds Européen de la Défense
- BPI France
- Budget National
- Ministère des Armées

Fonds Européen de la Défense

Suivi de la Réglementation

En Quoi Consiste NIS 2

- Extension du champ d'application
- Exigences renforcées de sécurité
- Coordination accrue entre États membres
- Obligations de notification des incidents
- Support et accompagnement

Comment Appliquer NIS 2

- ✓ Évaluation Initiale
- ✓ Mise en place de mesures de sécurité
- ✓ Développement de Plans de Continuité d'Activité
- ✓ Coopération avec les autorités nationales

Comment financer NIS 2 dans son entreprise ?

bpifrance

Cyber PME

FRANCE 2030

LOIRE VALLEY DATA HUB

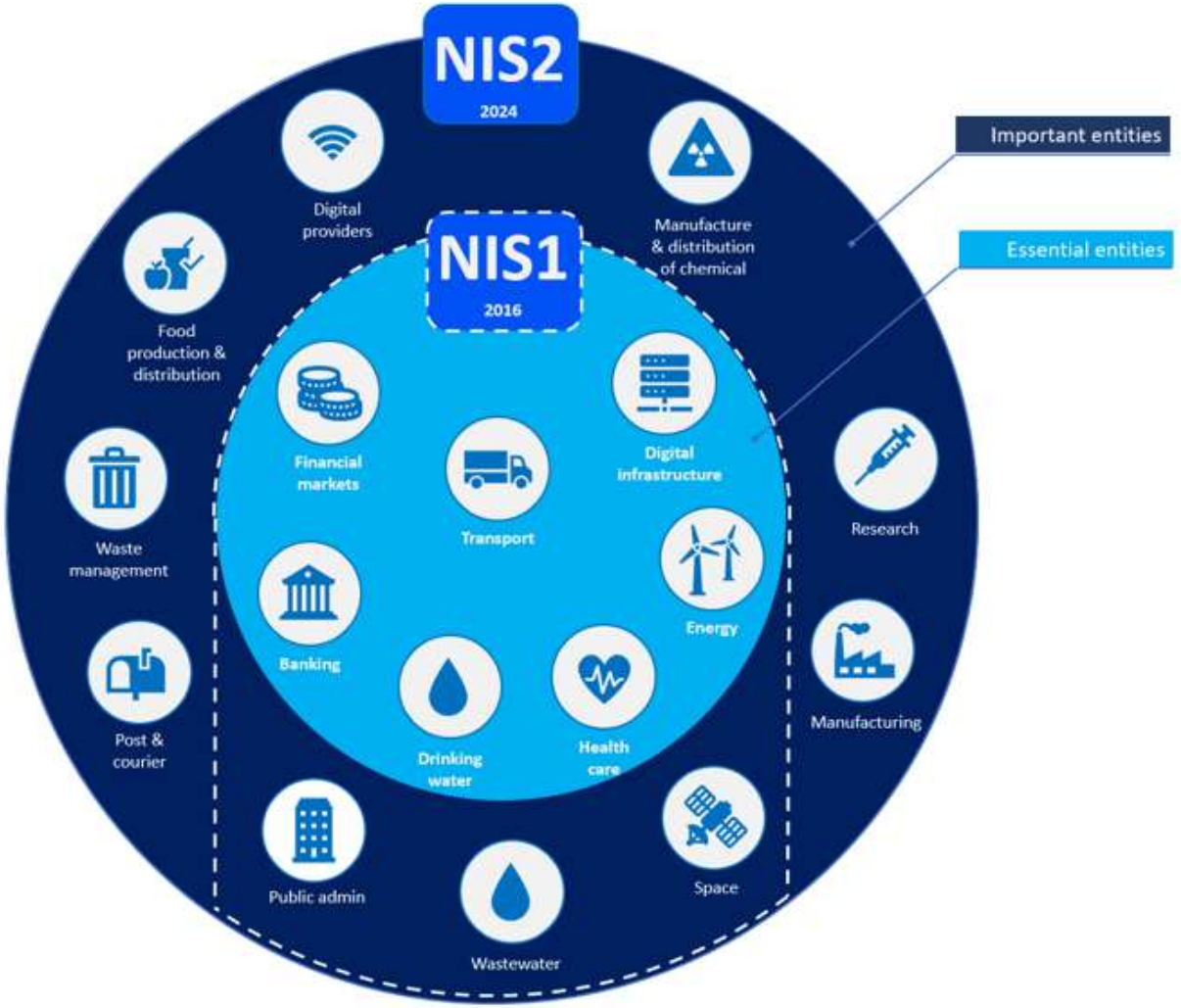
devup Centre-Val de Loire

NCC-FR
FRANCE CYBERSECURITY COORDINATION CENTRE

aftec formation

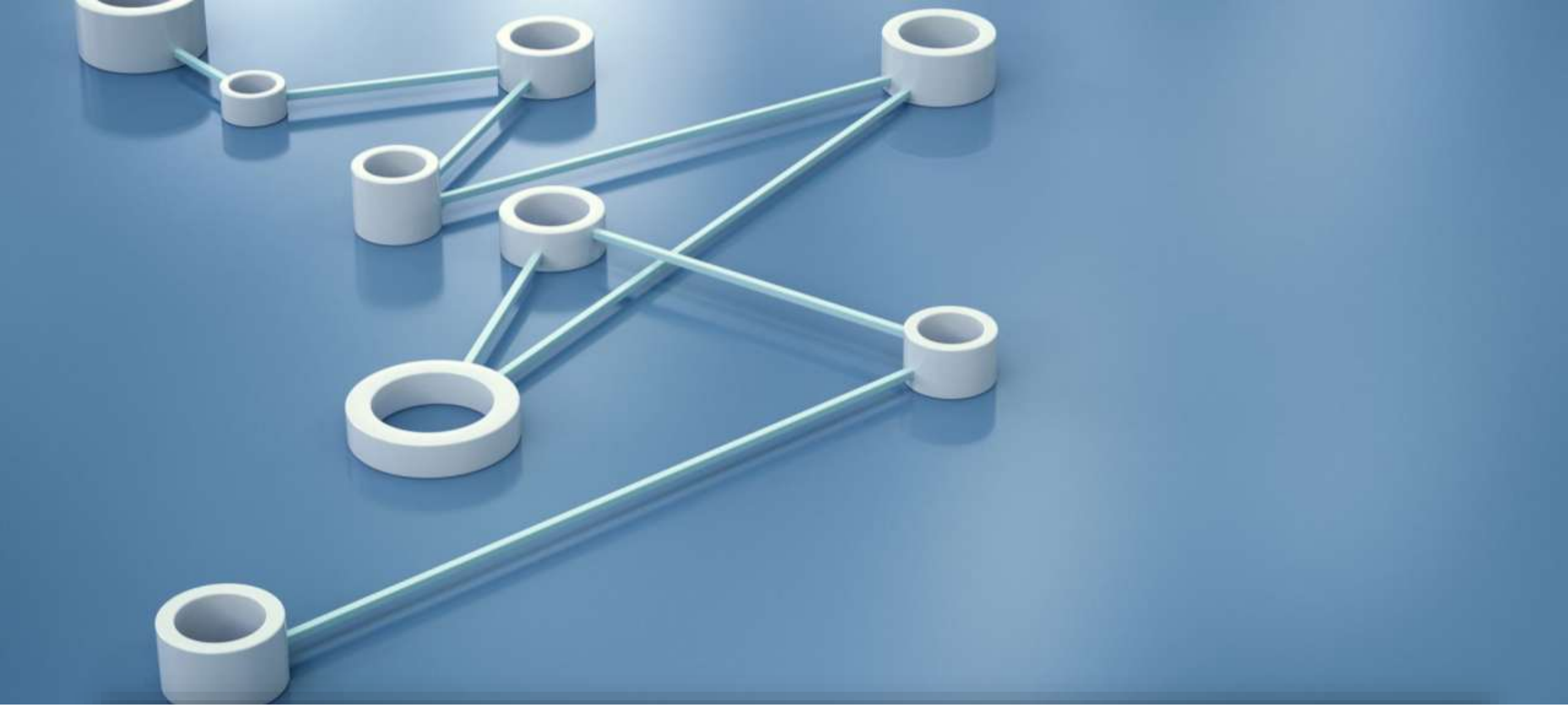
Ce qui va Changer avec NIS 2

- Inclusion de nouveaux secteurs
- Normes de sécurité plus strictes
- Amélioration de la résilience opérationnelle
- Augmentation des sanctions en cas de non-conformité


NIS2
2024
NIS1
2016
Important entities
Essential entities
Digital providers
Manufacture & distribution of chemical
Food production & distribution
Waste management
Post & courier
Research
Manufacturing
Space
Public admin
Wastewater
Drinking water
Health care
Banking
Financial markets
Transport
Digital infrastructure
Energy

NIS vs NIS 2

La Cyber
en France et Europe



Communication et évènementiel

European Cyber Week

by CYBER

MOIS EUROPÉEN DE LA CYBERSÉCURITÉ

Du 1er au 31 octobre 2018 #TousSecNum

HACK N' FLAG

INCYBER FORUM EUROPE

The 16th InCyber Forum at Lille Grand Palais

MARCH 26-28, 2024

CYBER MOIS

cybeRéponse

2ÈMES ASSISES RÉGIONALES DE LA CYBERSÉCURITÉ

20 mars 2024

9h-17h30

CHARTRES

aftec formation

CLUSIR Nord de France

CLUSIR Nouvelle-Aquitaine

CLUSIR OCCITANIE MÉDITERRANÉE

CLUSIR Normandie

CLUSIR BRETAGNE

CLUSIR Sud Provence Alpes Côte d'Azur

aftec formation

CAMPUS CYBER

HAUTS-DE-FRANCE • LILLE MÉTROPOLE

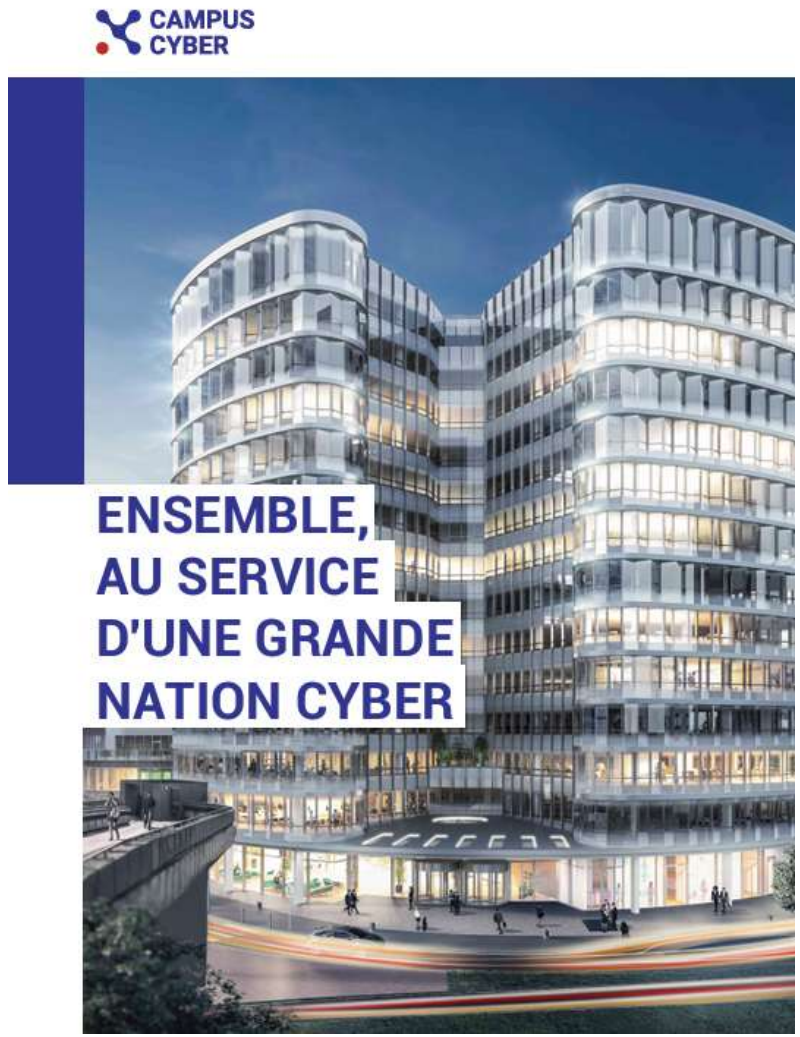
C3 CAMPUS RÉGIONAL DE CYBERSÉCURITÉ ET DE CONFIANCE NUMÉRIQUE

Nouvelle-Aquitaine

CAMPUS NORMANDIE CYBER

BRETAGNE Cyber Alliance

Le campus cyber breton



aftec formation

Répondre à la menace
Les cyber-pompiers

CSIRT-ATLANTIC

CENTRE CYBER
DU PACIFIQUE

CSIRT
HAUTS-DE-FRANCE

CSIRT
LA RÉUNION
COMPUTER SECURITY INCIDENT RESPONSE TEAM
Opéré par CYBER RÉUNION

NORMANDIE CYBER
CENTRE DE RÉPONSE AUX INCIDENTS CYBER

Grand Est Cybersécurité
CENTRE D'ASSISTANCE DE PROXIMITÉ

Urgence Cyber
îledeFrance
Centre de réponse aux cyberattaques

Breizh Cyber

CSIRT
BOURGOGNE-FRANCHE-COMTÉ

cybeRéponse
CENTRE-VAL DE LOIRE

C3RIC
CENTRE DE RÉPONSE AUX INCIDENTS CYBER
Nouvelle-Aquitaine

CYBER'OCC
LE CENTRE CYBERSÉCURITÉ EN OCCITANIE

Urgence Cyber
région Sud

CYBER CORSICA
CSIRT

aftec formation

CERT Crédit Mutuel EURO-INFORMATION

COMPUTER EMERGENCY RESPONSE TEAM CERT-AG CREDIT AGRICOLE

Caisse des Dépôts GROUPE CERT CDC INFORMATIQUE

Cyber Security Operation Center Security Data Network

AIRBUS CERT

CYBERSECURITE CERT SNCF Computer Emergency Response Team

Airbus, Areva, Bouygues, La Poste, Michelin, Orange, RATP, SNCF, Sopra Steria, Thales, Intrasec,

Axa, Crédit Agricole, Banque de France, BNP, Caisse des dépôts et consignations, BPCE, Société Générale

aftec formation


CERT [ED]


CERT
Aviation France


RENATER
CONNECTEUR DE SAVOIRS


FRANCE CYBER MARITIME
M-CERT


AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici
CERT
Santé


CERT-IST
INDUSTRIE | SERVICES | TERTIAIRE

TF-CSIRT

CERT-FR

signal spam

17 CYBER
Mon assistance en ligne

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

POLICE JUDICIAIRE
THESEE

PERCEV@L

PHAROS

aftec formation

corps d’armées et systèmes judiciaire


COMCYBERGEND


GENDARMERIE NATIONALE
UNC
UNITÉ NATIONALE CYBER


BRIGADE
numérique
Gendarmerie


GENDARMERIE NATIONALE
C3N
CENTRE DE LUTTE CONTRE LES CRIMINALITÉS NUMÉRIQUES


CYBERGEND
C-NTECH
INVESTIGATION & CRIMINALISTIQUE


GENDARMERIE NATIONALE
CYBERGEND
ENQUÊTEUR TECHNOLOGIES NUMÉRIQUES


ENQUÊTEUR TECHNOLOGIE NUMÉRIQUE
N-TECH
GENDARMERIE NATIONALE


CyberGendMar

COMCYBER – GROUPEMENT DE LA CYBERDÉFENSE DES ARMÉES

CALID
CENTRE D'ANALYSE EN LUTTE INFORMATIQUE DÉFENSIVE

COMCYBER – GROUPEMENT DE LA CYBERDÉFENSE DES ARMÉES

CASSI
CENTRE D'AUDITS DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

COMCYBER – GROUPEMENT DE LA CYBERDÉFENSE DES ARMÉES

CHIPI
CENTRE DES HOMOLOGATIONS PRINCIPALES INTERARMÉES

COMCYBER – COMMANDEMENT DE LA CYBERDÉFENSE

C2PO
CENTRE CYBER DE PRÉPARATION OPÉRATIONNELLE

COMMANDEMENT DU MINISTÈRE DE L'INTÉRIEUR

COMCYBER-MI

01000011 01001111 01001101
01000011 01011001 01000010
01000101 01010010
00101101 01001101
01001001

DANS LE CYBERESPACE

aftec formation

DEUX **COMCYBER** POUR DEUX MISSIONS DISTINCTES

COMCYBER

Commandement de la cyberdéfense des armées

COMCYBER-MI

Commandement du ministère de l'Intérieur dans le cyberespace

Notre raison d'être

- Combattre dans le cyberespace
- Lutter contre la cybercriminalité

Nos domaines d'action

- Défendre les systèmes d'information et systèmes d'armes de l'armée française ;
- Renseigner et agir sur les systèmes adverses ;
- Lutter contre la manipulation de l'information dans le cyberespace, sur les théâtres d'opérations extérieurs.
- Renseigner sur les structures cybercriminelles, leurs modes d'action et les modalités de blanchiment ;
- Participer à des opérations judiciaires dans un cadre partenarial et international ;
- Concevoir les outils juridiques et techniques.

Nos équipes

- Un commandement interarmées et des unités cybercombattantes des armées
- Un commandement ministériel et des unités spécialisées au sein des forces

Nos engagements communs

Partager la connaissance de la menace et des acteurs malveillants

MI

EUROPEAN CYBERCRIME TRAINING & EDUCATION GROUP

ECTEG

EUROPOL

EC3 | European Cybercrime Centre

JOINT CYBERCRIME

J-CAT

ACTION TASKFORCE

EUROPEAN JUDICIAL

E01000101

J01001010

C01000011

N01001110

CYBERCRIME NETWORK

PARQUET DE PARIS

JUNALCO

EUROJUST

aftec formation

Communauté cyber française

LID = Lutte informatique défensive
LIO = Lutte informatique offensive

LID = Lutte informatique défensive

DIRCAB PM
CNRLT
CEMP
SGDSN
Min X
Comité directeur de la cyberdéfense

PREMIER MINISTRE

DIRCAB PM
ANSSI
Min X
Comité de pilotage de la cybersécurité

C4 STRAT
C4 TECH
C4 TECHOPS
Centre de coordination des crises cyber C4

MINISTÈRE DES ARMÉES

MINISTÈRE DE L'INTÉRIEUR

Le COMCYBER assure la protection des systèmes d'information placés sous la responsabilité du chef d'état-major des armées en sa qualité d'autorité qualifiée pour la sécurité des systèmes d'information et la conduite de la défense du ministère des Armées.

Au sein de la DRM, le Centre de recherche et d'analyse cyber concourt à informer, éclairer, renseigner les autorités dans leurs décisions, notamment relatives aux opérations sur théâtres extérieurs.

Agence nationale de la sécurité des systèmes d'information (ANSSI)

Rôles : anticipation, détection de la menace, réponse aux incidents. Opération de cyberdéfense ouverte à ce niveau. Sous-direction des opérations (SDO) : assure au niveau opératif et tactique la défense des systèmes numériques d'intérêt pour la nation.

Renseignements

DGA

Direction générale de l'armement (DGA)

La DGA est le maître d'ouvrage des programmes d'armement. La DGA-Maîtrise de l'information (DGA-MI) est en charge de concevoir les armes cybernétiques au profit du ministère des Armées, que ce soit pour les services de renseignement où pour les forces du COMCYBER.

COMCYBER

Commandement de cyberdéfense (COMCYBER)

Pour l'exercice de ses missions, le COMCYBER dispose d'un état-major et a une autorité sur trois organismes interarmées : CALID, CASSI et CPROC.

DRM

Direction du renseignement militaire (DRM)

DRSD

Direction du renseignement et de la sécurité de la Défense

DGSE

Direction générale de la sécurité extérieure (DGSE)

DGSE et DRSD assurent eux-mêmes la protection de leurs systèmes d'informations, en plus de leurs activités de renseignements s'agissant des menaces et enjeux du secteur de la défense.

Tracfin

Cellule française de lutte contre le blanchiment de capitaux et le financement du terrorisme

DNRED

Direction Nationale du Renseignement et des Enquêtes Douanières (DNRED)

DGSIS

Direction générale de la Sécurité intérieure (DGSIS)

Tracfin dispose d'une division d'enquête spécialisée sur la cybercriminalité financière, tandis que la DNRED dispose d'un service spécialisé : Cyberdouane.

Prévention, surveillance et répression des actes d'ingérence portant atteinte au potentiel économique, industriel et scientifique du pays.

Réserve citoyenne de cyberdéfense (RCC)

Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI)

Rattaché à la préfecture de police de Paris, elle lutte contre la cybermenace à Paris et en petite couronne. Elle traite principalement des atteintes aux systèmes de traitement automatisés de données.

C3N

Centre de lutte contre les criminalités numériques (C3N)

Rattaché au pôle judiciaire de la gendarmerie nationale (PJGN), est chargé d'identifier les phénomènes émergents et de conduire des investigations d'initiative sur internet. Il coordonne également le réseau des enquêteurs technologies numériques (NTECH) et leurs correspondants (C-TECH).

Sous-direction de la Lutte contre la Cybercriminalité (SDLC)

Rattaché à la Direction centrale de la police judiciaire (DCPJ), elle est en charge du pilotage et de la coordination de la lutte contre la cybercriminalité au plan national. Elle détecte les nouvelles menaces, aide les victimes et enquête afin de réprimer les crimes. Pharos et Info escroqueries sont des plateformes de l'office central de lutte contre la criminalité liée aux technologies de l'information de la communication (OCLCTIC).

INHESJ
INSTITUT NATIONAL DES HAUTES ÉTUDES DE LA SÉCURITÉ ET DE LA JUSTICE

Revue Stratégique de cyberdéfense de 2018

Livre Blanc Défense et Sécurité nationale de 2013

Document réalisé par Martial Le Guédard,
Département Risques & Crises

GESTION DE CRISE & CHAÎNES CYBER : SYNTHÈSE DE L'ORGANISATION EUROPÉENNE ET FRANÇAISE LIÉE À LA SÉCURITÉ NUMÉRIQUE

DISPOSITIFS CYBER

Organisation du Traité de l'Atlantique Nord OTAN

Le Conseil de l'Europe aide à protéger les sociétés contre les menaces de la cybercriminalité via la **Convention de Budapest**, qui reste encore aujourd'hui le cadre juridique international contraignant de référence pour les différentes législations nationales, mais aussi via son comité de la convention sur la cybercriminalité (**T-CY**) ou encore son bureau du programme sur la cybercriminalité (**C-PROC**).

Conseil de l'UE

Le Commission a adopté en 2017 une recommandation : le **Blueprint**, définissant les procédures de coopération et d'échanges européens pour la gestion des incidents majeurs et des crises cyber. La commissaire au marché intérieur est en charge du renforcement de la cybersécurité de l'Europe, la sécurité des réseaux et des systèmes d'information, des mécanismes d'urgence en cas de cyber-incident et le déploiement de l'outil commune pour la cybersécurité (Joint Cyber Unit).

L'Alliance a pour principale fonction la défense collective, la gestion de crise et la sécurité coopérative. Des équipes de réaction rapide de l'OTAN peuvent intervenir 24 h/24 au nom de la clause d'assistance mutuelle de l'article 5 du traité de l'Atlantique nord (TAN).

La NATO Communications and Information Agency (NCIA), fournit aux pays de l'Alliance les moyens de communiquer. Elle est autant l'agence unique d'acquisition des moyens que l'opérateur interne Cyber de l'OTAN. La NCIRC lui est rattaché.

NCI AGENCY

NCIRC

La Capacité OTAN de réaction aux incidents informatiques, la NCIRC coopère étroitement avec le CERT-EU. Forte de quelques 200 experts, elle assure la protection des SI de l'Alliance en temps de paix et en temps de crise. D'ici 2023, un Centre des cyberopérations (CyOC) devrait être également intégré à la structure de commandement de l'OTAN.

CCDCOE

Le Centre d'excellence de cyberdéfense coopérative, basé à Tallinn est le centre de l'OTAN spécialisé dans la recherche et l'éducation en élaborant notamment les règles de comportement dans le cyberespace et notamment la question de l'applicabilité du droit international aux cyberattaques employées dans le cadre de conflits armés via le "**Manuel de Tallinn**". Les exercices européens de cybersécurité de l'OTAN: Cyber Coalition et Locked Shields y sont organisés.

En cas de crise ou incident majeur, la coordination pourra s'effectuer dans le cadre du système d'alerte rapide « **ARGUS** » au sein de la Commission, tandis que le Conseil de l'UE assurera la coordination politique via le dispositif intégré pour une réaction au niveau politique dans les situations de crise (**PCIR**). Enfin, lorsque la crise comporte d'importantes implications liées à la politique extérieure ou à la politique de sécurité et de défense commune (**PSDC**), le système de réponse aux crises (SRC) du Service européen pour l'action extérieure (**SEAE**) pourra être activé, tout comme les services de renseignement, INTCEN et EUMS INT, dans le cadre de la capacité unique du renseignement (SIAC).

L'État-major de l'UE (EMUE), structure militaire intégrée à l'UE, est en mesure de fournir une expertise militaire et opérationnelle via sa division politique et plans (CON/CAP) et sa division des systèmes d'information et de commandement (C3I). Mais ce sont les structures de planification européennes qui ont la charge de la conduite opérationnelle cyber dans les opérations ou le **MPCC** pour les opérations à mandat non exécutif.

Union Européenne ACTION EXTÉRIEURE

CSIRTs

Le "**CERT-EU**", Computer Emergency Response Team de l'UE intervient en cas d'urgence informatique via une équipe permanente au profit des institutions européennes. Il coopère notamment avec les CERTS des États membres. Le **CSIRTs Network** est le réseau des CERT européens.

L'Agence européenne de la sécurité des réseaux et de l'information (**ENISA**) consulte et assiste la Commission et les États membres en matière de sécurité de l'information. Son rôle se renforce, notamment en matière de certification et d'organisation d'exercices.

enisa European Network and Information Security Agency

Europol est l'agence européenne spécialisée dans la répression de la criminalité internationale et le terrorisme. Elle lutte contre la cybercriminalité, notamment via l'European Cybercrime Centre (**JCX**) qui opère à un niveau stratégique mais également opérationnel, notamment via le Joint Cybercrime Action Taskforce (**J-CAT**).

EUROPOL EC3 European Cybercrime Centre

EUROJUST

L'European Union Agency for Criminal Justice Cooperation (Eurojust) a pour principales missions la coordination des enquêtes et des poursuites, et la coopération entre les autorités des États membres. Elle cherche à rendre plus efficaces les enquêtes et poursuites, notamment en matière de lutte contre la cybercriminalité.

EJCN

Soutenu par Eurojust, L'European Judicial Cybercrime Network (**EJCN**) forme un réseau de procureurs et de spécialistes du cybercrime. Il vise à rendre plus efficace les enquêtes et poursuites engagées en matière de cybercrime en améliorant la coopération entre autorités judiciaires des États membres.

Comité directeur de la cyberdéfense

Comité de pilotage de la cybersécurité

PREMIER MINISTRE

SGDSN

CIC

Centre de coordination des crises cyber CO

Agence nationale de la sécurité des systèmes d'information (ANSSI)

Le Centre de Cyberdéfense (C2MI) relevant du SHFD assure la défense des SI du ministère de l'intérieur. Il assure la détection des attaques et coordonne la gestion des incidents de sécurité en lien avec l'ANSSI.

Le MEAE assure le lien avec les homologues étrangers. Il s'appuie sur son Centre de crise et de soutien (CDCS), la Cellule interministérielle d'aide aux victimes (CIAV), mais également le réseau de diplomates en ambassades et consulats.

La cellule de crise JUSTICE est animée par le HFDS qui est responsable de la sécurité et la résilience du secteur d'activités d'importance vitale des activités judiciaires (SAIVAJ).

La COBER, est le centre opérationnel de Bercy, mis en œuvre par le service du Haut Fonctionnaire de défense et de sécurité. Il conduit l'action du réseau de gestion de crise des ministères économiques et financiers. Si la crise a un fort impact sur la vie économique de la Nation, le ministre de l'économie et des finances décide de mettre en œuvre la cellule de continuité économique (CCE).

Le FSSI des ministères sociaux pilote la cellule d'Accompagnement Cybersécurité des Structures de Santé « (ACSS), structure nationale d'assistance et d'appui pour les ARS et autres structures de santé. Le FSSI peut compter sur l'agence du numérique en santé et le portail https://www.cyberveille-sante.gouv.fr/. Les signalements remontent également des ARS vers l'ASIP Santé via l'ACSS et notamment grâce au portail signalement.social-sante.gouv.fr.

COGIC FSSI COPN C2MI CROGEND

CDCS CIAV FSSI

JUSTICE DIAV CISV FSSI

COBER CCE FSSI

CORRUSS DGS FSSI ACSS

CPCO FSSI

Rattachée à l'État-major des Armées (EMA), il faut souligner le rôle de la Direction interarmées des réseaux d'infrastructure et des systèmes d'information (**DIRISI**) qui est un service interarmées, son centre d'exploit de la sécurité des systèmes d'information (CASSI) et le SOC DIRISI sont notamment impliqués dans la défense des SI du ministère des Armées, qu'elle conçoit, développe et protège.

La DIRISI appuie le CPCO sur ses opérations, mais également les 3 armées et les autres directions et organismes.

Le CCO évalue le niveau de menace dans le but de fixer ensuite le stade d'alerte de la chaîne défensive dans le cadre de la posture permanente de cybersécurité (PPC). L'officier général commandant de la cyberdéfense (OGC/CYBER) fixe le stade d'alerte à adopter par la chaîne défensive, en lien avec le SCOPS de l'EMA et le HFCDS.

Au sein de la DRM, le Centre de recherche et d'analyse cyber concourt à informer, éclairer, renseigner les autorités dans leurs décisions, notamment relatives aux opérations sur théâtres extérieurs.

DRSSI et DRSD assurent elles-mêmes la protection de leurs systèmes d'information, en plus de leurs activités de renseignement s'agissant des menaces en anjeux du secteur de la défense. La DRSD a également la responsabilité de la partie cybersécurité concernant les SI consommé à la dissuasion.

DRM

Direction du renseignement militaire (DRM)

Direction générale de la sécurité extérieure (DGSE)

Direction du renseignement et de la sécurité de la Défense (DRSD)

État-major des Armées

DGA

Direction générale de l'armement (DGA)

SGA

Secrétariat général pour l'administration

RZSSI COZ

Liberté • Égalité • Fraternité RÉPUBLIQUE FRANÇAISE

SGZDS

COD RSSI

Liberté • Égalité • Fraternité RÉPUBLIQUE FRANÇAISE

PREFECTURE

RSSI PCO

Liberté • Égalité • Fraternité RÉPUBLIQUE FRANÇAISE

MAURIE

Commandement de cyberdéfense (COMCYBER)

La DGA est le maître d'ouvrage des programmes d'armement. La DGA-Maîtrise de l'information (**DGA-MI**) est en charge de concevoir les armes cybernétiques au profit du ministère des Armées, que ce soit pour les services de renseignement ou pour les forces du COMCYBER, elle peut également appuyer le GCA/CAUD ou être chargée de certaines tâches d'expertise technique, notamment via son pôle SSI.

Le COMCYBER assure la protection des systèmes d'information placés sous la responsabilité du chef d'état-major des armées en sa qualité d'autorité qualifiée pour la sécurité des systèmes d'information et la conduite de la défense du ministère des Armées. Pour l'exercice de ses missions de **lutte informatique défensive (LID)**, le COMCYBER dispose d'un état-major et d'un centre cyber opérationnel (CCO) et a une autorité sur différents organismes spécialisés.

Le groupement cyberdéfense des armées (GCA) qui regroupe le GCA/CAUD, GCA/CRPOC, GCA/CASSI , les groupements d'intervention cyber (GIC) et SOC. À noter également : les activités de **lutte informatique Offensive (LIO)** désignant l'ensemble des actions entreprises dans le cyberespace visant à produire des effets à l'encontre d'un système adversa, pour en altérer la disponibilité ou la confidentialité des données.

PÔLE D'EXCELLENCE CYBER

Pôle d'Excellence Cyber (PEC) et CyberDefense Factory, sont deux exemples qui témoignent de l'importance du partenariat public-privé en matière de cybersécurité et cyberdéfense. Sans oublier la convention: cyber impliquant 8 grands mailles d'assure industriels et principaux équipementiers du ministère afin de construire une chaîne cyber défensive « de tout en tout ».

La 807ème compagnie de Transmissions (807e CTRS), est une compagnie spécialisée en LID. Placée sous l'autorité fonctionnelle conjointe de l'armée de Terre (mission Terre) et du COMCYBER (mission RIMA). Elle contribue à la LID en opération.

ARMÉE DE TERRE

L'ensemble des états-majors, directions et services (EMDS) rattachés au ministère des Armées, wonnent chacun une chaine SSI et LID. Placés sous l'autorité fonctionnelle d'un OSCYBER (OSCYBER Terre, Air, et ALCYBER pour la Marine). Les 3 armées disposent de centres techniques dédiés **ESOC** pour l'armée de l'Air, **CSC** pour la Marine, CTUD pour l'Armée de Terre) et de SOC travaillent en étroite collaboration avec le GCA/CAUD et en mesure d'armer des GIC.

Service de santé des armées

MARINE NATIONALE

ADIRISI

ARMÉE DE L'AIR

Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI)

Rattachée à la préfecture de police de Paris, elle lutte contre la cybermenace à Paris et en petite couronne. Elle traite principalement des attentes aux systèmes de traitement automatisés de données.

Prestataire de réponse aux incidents de sécurité qualifiés (PRIS)

Le secteur privé est fortement impliqué en matière de défense des SI, en témoignent le mise en place de la qualification des prestataires de réponse aux incidents de sécurité qualifiés (PRIS) par l'ANSSI, mais également le dispositif national

CYBERMALVEILLANCE.GOUV.FR de prévention du risque numérique et d'assistance aux victimes piloté par le GIP ACYMA qui permet le mise en relation entre victimes (TPE/PME et citoyens) et services professionnels de sécurité informatique ou bien la Brigade du numérique (BNUM) de la gendarmerie nationale. À noter la naissance du label pour la reconnaissance des services en sécurité informatique et le rôle de la recherche dans le développement des capacités de réponse.

Sous-direction des opérations (SDO) assure au niveau opérationnel et tactique la défense des systèmes numériques d'intérêt pour la nation. Le **CERT-FR** est le CERT national, il est le point de contact international privilégié pour tout incident de nature cyber touchant la France. Il assure une permanence de ses activités 24h/24, 7j/7.

Rôles : anticipation, détection de la menace, réponse aux incidents. Opération de cybersécurité ouverte à ce niveau.

Sous-direction de la Lutte contre la Cybercriminalité (SDLC)

Rattachée à la Direction centrale de la police judiciaire (DCPJ), elle est en charge du pilotage et de la coordination de la lutte contre la cybercriminalité au plan national. Elle détecte les nouvelles menaces, aide les victimes et enquête afin de réprimer les crimes.

Division Analyse & Anticipation

Le C3NAT-POLICE JUDICIAIRE est rattachée à la SDJA.

Office central de lutte contre la criminalité liée aux technologies de l'information de la communication (OCLCTIC)

L'OCLCTIC gère PHAROS et THESEE.

Centre de lutte contre les criminalités numériques (C3N)

Rattaché au pôle judiciaire de la gendarmerie nationale (PJGN), est chargé d'identifier les phénomènes émergents et de conduire des investigations d'initiative sur internet.

Le C3N coordonne également le réseau CyberGEND, composé d'enquêteurs technologues numériques (NTECH), de correspondants (C-TECH) et de primo-intervenant (P-NTECH).

Direction générale de la Sécurité intérieure (DGSI)

Prévention, surveillance et répression des actes d'ingérence portant atteinte au potentiel économique, industriel et scientifique du pays.

Elle possède un rôle en matière judiciaire, mais également en matière de défense des SI des OIV, OSE et des réseaux gouvernementaux.

Si cas d'une attaque qualifiée de terroriste, le parquet de Paris peut saisir la sous-direction anti-terroriste (SDAT), qui dispose d'une compétence judiciaire nationale.

SDAT

Tribunal judiciaire de Paris

La Section 23 Cybercriminalité du Parquet de Paris est l'une des trois juridictions interrégionales spécialisées (JIRS) au côté de la section 15 JIRS criminalité organisée et la section 32 JIRS criminalité financière. Cette division comprend de 3 magistrats est en charge des contentieux de très haut vol, de complexe à très complexe, comme ceux relatifs à WannaCry et NotPetya.

La section 23 s'appuie également sur quatre juges d'instruction du pôle financier de Paris formés aux problématiques cyber.

Direction Nationale du Renseignement et des Enquêtes Douanières (DNRED)

La DNRED dispose d'un service spécialisé : Cyberdouane.

Cellule française de lutte contre le blanchiment de capitaux et le financement du terrorisme

Tracfin dispose d'une division d'enquête spécialisée sur la cybercriminalité financière.

Un réseau de magistrats « cyber-référents » opèrent au sein des tribunaux, cours d'appel et JIRS. La Mission de lutte contre la cybercriminalité de la direction des affaires criminelles et des grâces (DACG) du ministère de la justice contribue aux travaux stratégiques du CA mais également aux réunions du Groupe de Contact permanent (GCP), piloté par la DNRSC.

La Police et la Gendarmerie nationale ont développé des plateformes dédiées à la prise en compte des incidents cyber pour les collectivités, les TPE et PME et les particuliers.

THESEE

PERCEVAL

INHESJ INSTITUT NATIONAL DES HAUTES ÉTUDES DE LA SÉCURITÉ ET DE LA JUSTICE

DISPOSITIFS DE CRISE

FSSI = Fonctionnaire de la sécurité des systèmes d'information, nommé par le HFDS
RSSI = Responsable zonal de la sécurité des systèmes d'information
RSSI = Responsable de la Sécurité des systèmes d'information

Infographie réalisée par Martial LE GUÉDARD
Consultez l'article en cliquant ici.

THE SITE IS NOW UNDER CONTROL OF LAW ENFORCEMENT

This site is now under the control of The National Crime Agency of the UK, working in close cooperation with the FBI and the international law enforcement task force, 'Operation Cronos'.

We can confirm that Lockbit's services have been disrupted as a result of International Law Enforcement action – this is an ongoing and developing operation.

Return here for more information at:

11:30 GMT on Tuesday 20th Feb.

NCA National Crime Agency
SOUTH WEST ROCU
METROPOLITAN POLICE
EUROPOL
POLITIE
Kanton Zürich
Gendarmerie
SH Schleswig-Holstein
POLIISI
AUSTRALIAN FEDERAL POLICE

THIS WEBSITE HAS BEEN SEIZED

OPERATION COOKIE MONSTER

Genesis Market's domains have been seized by the FBI pursuant to a seizure warrant issued by the United States District Court for the Eastern District of Wisconsin. These seizures were possible because of international law enforcement and private sector coordination involving the partners listed below.

To determine if you have been victimized, visit:
haveibeenpwned.com or politie.nl/checkyourhack

Been active on Genesis Market? In contact with Genesis Market administrators?
Email us, we're interested: FBIMW-Genesis@fbi.gov

POLITI
AFP
CBZC
GUARDIA CIVIL
NCA National Crime Agency
Federal Criminal Police Office
EUROPOL
EUROJUST
POLIISI KESKUSRIKOSPOLIISI Centralkriminalpolisen National Bureau of Investigation
POLITIE
Polisen Swedish Police
Qintel

Géopolitique

CSIRTs NETWORK

computer emergency response team
CERT-EU
for the EU institutions, bodies and agencies

NIS COOPERATION GROUP

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

NCC-FR
FRANCE CYBERSECURITY COORDINATION CENTRE

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
RESOURCE CENTRE ON CYBERJUSTICE AND ARTIFICIAL INTELLIGENCE

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

aftec formation

CCDCOE

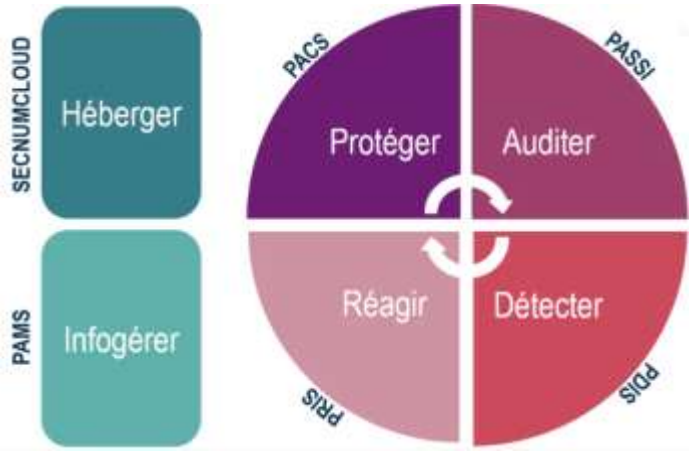
NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

NATO Communications and Information Agency
Agence OTAN d´information et de communication

Industrie & services

diagonal → MonAide Cyber
INNOVATION ANSSI

RÉFÉRENCÉ SUR LA PLATEFORME
CYBERMALVEILLANCE.GOUV.FR
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité
CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique



VISA DE SÉCURITÉ
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr
RÉPUBLIQUE FRANÇAISE

aftec formation


PROFESSIONNEL LABELLISÉ EXPERTCYBER
PROFESSIONNEL RÉFÉRENCÉ SUR CYBERMALVEILLANCE.GOUV.FR
INSTALLATION MAINTENANCE ASSISTANCE
PÉRIMÈTRE ÉLIGIBILITÉ
ASSISTANCE
PROFESSIONNELS (TPE, PME, COLLECTIVITÉS, ASSOCIATIONS...)
PUBLIC
PARTICULIERS ET/OU PROFESSIONNELS (TPE, PME, COLLECTIVITÉS, ASSOCIATIONS...)
COMPÉTENCES VÉRIFIÉES SUR LA BASE D'UN AUDIT AFNOR
CRITÈRES D'ÉVALUATION DES COMPÉTENCES
AUTO-DÉCLARATIF
2 ANS, RENOUVELABLES
VALIDITÉ DU STATUT
DURÉE INDÉTERMINÉE*
SÉCURISATION EN AMONT ET INTERVENTION SUR INCIDENT
MISE EN RELATION
INTERVENTION SUR INCIDENT

ISO/IEC 27001 :
Sécurité de l’information

ISO/IEC 27002 :
Bonnes pratiques de gestion de la sécurité de l’information

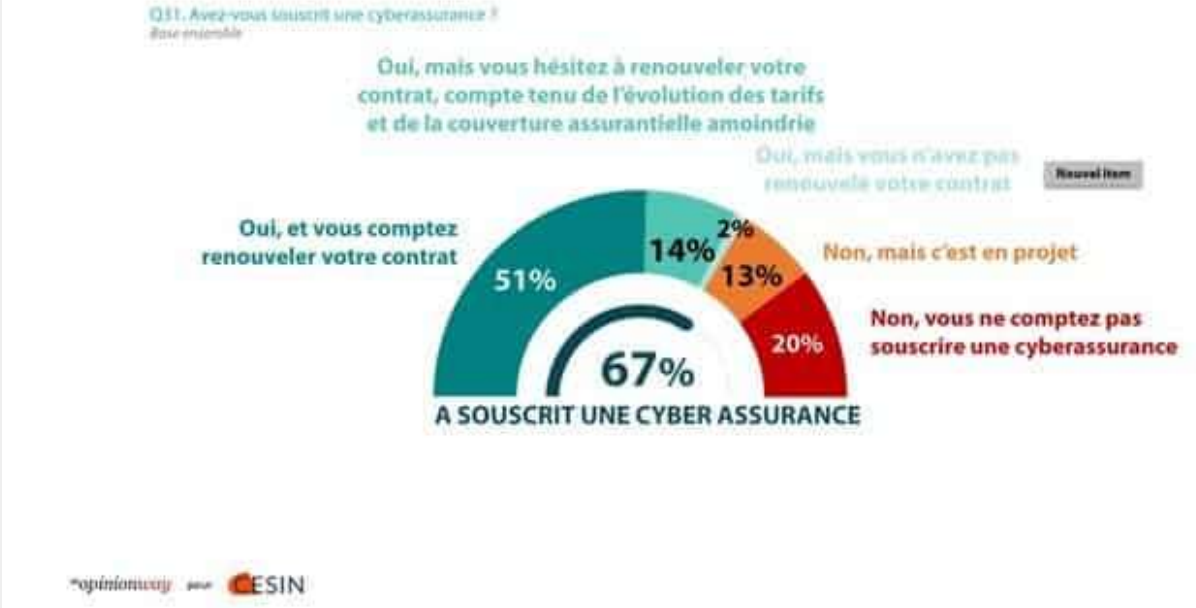
ISO/IEC 27005 :
Gestion des risques liés à la sécurité de l’information

ISO/IEC 27701 :
Gestion des informations personnelles (PII)

ISO/IEC 27017 :
Sécurité de l’information dans le cloud

ISO/IEC 27018 :
Protection des données personnelles dans le cloud

Assurances cyber-risques



CYBER BOOSTER

POWERED BY

CYGO ENTREPRENEURS

LE POOL × LA FRENCH TECH RENNES SAINT-MALO

PÔLE D'EXCELLENCE CYBER

EDIH European Digital Innovation Hubs Network

CYBER D3FENSE FACTORY

aftec formation

Pour aller plus loin

SENS CYBER
E-sensibilisation à la cybersécurité pour tous

SecNum académie
ANSSI

Sen Cy-Crise
Initiation à la gestion de crise cyber

CLUSIF
MEHARI & Club RSSI

L'ATELIER RGPD

EBIOS RISK MANAGER
Club EBIOS

aftec formation

En conclusion

- **Les réglementations en vigueur**
- **NIS 2, a quoi s'attendre ?**
- **La cyber en France et EU (évènementiel, cyber-pompiers, judicaire, géopolitique, industrie, etc..)**

Références :

✓ cyber.gouv.fr (ssi.gouv.fr)
✓ monespacenis2.cyber.gouv.fr
✓ francenum.gouv.fr
✓ Rapport Annuel sur la Cybercriminalité 2024 COMCYBERMI
✓ Rapport d'activité et état de la menace 2023 Cybermalveillance

aftec formation

APPRENTISSAGE SUPÉRIEUR ET FORMATION PROFESSIONNELLE

Clément TEISSIER