Webinaire du 25 juin 2026

Enjeux de Cybersécurité pour les entreprises de la filière Energie

MEDEE

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ANSSI

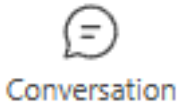
CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE

DGSI

NUCLÉI
Hauts-de-France

Rappel des consignes

Le webinaire est enregistré afin de permettre une rediffusion différée



Pour poser vos questions,
Merci d'utiliser le fil de discussion Teams ou de lever la main

Programme

1. Présentation des structures et correspondants

2. Présentation de la thématique : Enjeux de Cybersécurité pour les entreprises de la filière Energie

3. Questions / Réponses

4. Prochain webinaire

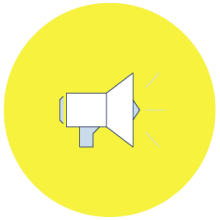
Présentation des structures et correspondants

Hugo LONGUESPÉ
Délégué à la sécurité numérique pour la région Hauts de France

Camille DESAUNOIS
Startup Manager Cybersécurité

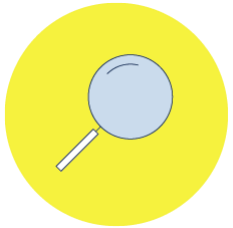
Valentin GRUSON
Analyste Cybersécurité

L'ANSSI
Agence nationale de la sécurité des systèmes d'information



Autorité nationale en matière de cybersécurité et de cyberdéfense créée en 2009

Service du Premier ministre placé sous l'autorité du secrétaire général de la défense et de la sécurité nationale (SGDSN)



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

Mission défensive (et non offensive)

Rôle : protéger la Nation face aux cyberattaques

Hugo LONGUESPÉ
Délégué à la sécurité numérique HDF
hauts-de-france@ssi.gouv.fr | 06 49 86 17 17

Le Campus Cyber HDFLM

CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE

Le Campus Cyber Hauts-de-France Lille Métropole fédère les acteurs privés et publics dans le domaine de la cybersécurité.

Il les sensibilise, les guide et les assiste.

Il favorise l'innovation, les compétences et les talents.

Il développe le secteur de la cybersécurité.

Bâtiment Wenov

177 allée Clémentine Deman

59000 Lille

campus@hdf.campuscyber.fr

https://hdf.campuscyber.fr

CSIRT HAUTS-DE-FRANCE

pour « Computer Security Incident Response Team »
ou « Équipe de réponse aux incidents de sécurité informatique »

- Web : **csirt-hdf.fr**

- Téléphone : **0806 700 111**

Valentin GRUSON
Analyste Cybersécurité

MEDEE

Maîtrise Energétique des Entraînements Electriques

- Le Pôle MEDEE est le cluster dédié à la **R&D et à l'Innovation** dans le domaine de **l'énergie électrique** en Hauts-de-France.

- **Savoir-faire :** accompagner les structures, de l'idée à la promotion de leurs projets, en passant par la recherche de financements et de partenaires en France et à l'international.

- **4 Marchés :**
  - Les réseaux électriques intelligents
  - Les énergies renouvelables
  - L'efficacité énergétique des process industriels
  - La mobilité électrique

Un Comité Scientifique

Composition paritaire entre membres académiques et industriels

- Axe 1 : Matériaux et composants
- Axe 2 : Convertisseurs d'énergie intelligents
- Axe 3 : Intégration système, Gestion et stockage
- Axe transverse : Outils & méthodes numériques

Besoin de booster un projet ?

Votre contact :

Sébastien DROUART, Directeur opérationnel
EuraTechnologies, place Pierre de Saintignon
165, avenue de Bretagne – 59000 Lille, France
06 22 06 06 57 | sdrouart@pole-medee.com
www.pole-medee.com

LE PROGRAMME DE DÉVELOPPEMENT ÉCONOMIQUE ET D'ACCOMPAGNEMENT DES ENTREPRISES RÉGIONALES DE LA FILIÈRE NUCLÉAIRE

NUCLÉI Hauts-de-France

nuclei.fr

contact@nuclei.fr

Les objectifs du programme

1. ***Faciliter l'accès aux marchés du nucléaire****, porteurs d'activité et d'emplois*
2. ***Accompagner*** *les entreprises régionales du secteur nucléaire et celles qui souhaiteraient intégrer ce secteur d'activité, en particulier dans leur prise en compte des exigences spécifiques de la filière (ISO 19443, certification radioprotection, …)*
3. ***Animer et valoriser*** *le réseau des entreprises régionales de la filière nucléaire*

CCI Business Hauts de France – Communauté NUCLEAIRE

Vos interlocuteurs

Magali TRIBONDEAU m.tribondeau@hautsdefrance.cci.fr

Philippe STAHL philippe.stahl@edf.fr

*NUCLÉI Hauts-de-France anime la **Communauté Nucléaire** de CCI Business Hauts-de-France*

pour recevoir notre lettre hebdo

Inscrivez-vous !

hautsdefrance.ccibusiness.fr/nucleaire

C'est gratuit !!!

Région Hauts-de-France – Cofinancé par l'Union européenne – CCI HAUTS-DE-FRANCE – EDF – CAP' INDUSTRIE – framatome – GIP NO – FRANCE CHAUDRONNERIE – CCI Business – Gifen – UNIVERSITÉ DES MÉTIERS DU NUCLÉAIRE – Nuclear Valley

Programme

1. Présentation des structures et correspondants

2. **Présentation de la thématique : Enjeux de Cybersécurité pour les entreprises de la filière Energie**

3. Questions / Réponses

4. Prochain webinaire

RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

WEBINAIRE CYBERSÉCURITÉ N°2

ENJEUX DE CYBERSÉCURITÉ POUR LES ENTREPRISES DE LA FILIÈRE ENERGIE

26 JUIN 2026

Hugo LONGUESPÉ
Délégué à la sécurité numérique
Hauts de France
hauts-de-france@ssi.gouv.fr

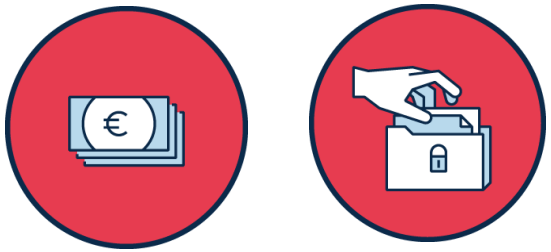
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

L'ÉTAT DE LA MENACE CYBER

État de la menace

Finalités des attaques

La finalité lucrative



Les attaques par rançongiciels.

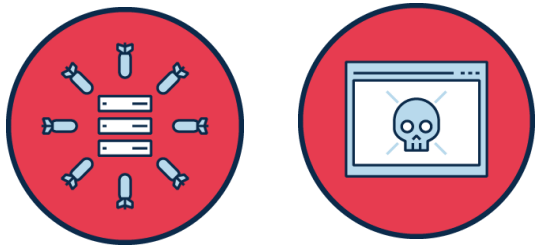
Les exfiltrations et ventes de données informatiques.

Les attaques d'ingénierie sociale comme les faux ordres de virement (FOVI), etc.

L’espionnage

Les vols d’informations stratégiques, notamment celles des entités gouvernementales, d’entreprises innovantes ou sensibles, etc.

Le sabotage et la déstabilisation



Des attaques menées par des groupes hacktivistes (DDOS, défiguration de sites internet, etc.).

Ou des groupes d’affiliation étatique : une logique de sabotage pour laquelle une vigilance s’impose.

Panorama de la cybermenace

Une menace systémique

- Lucrativité
- Déstabilisation
- Espionnage

Aux origines diverses

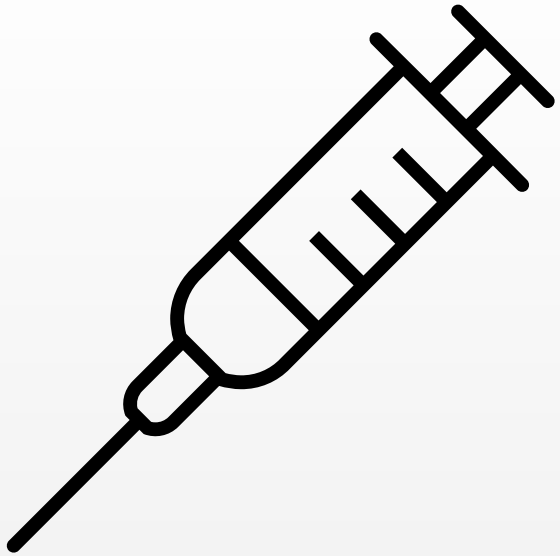
Cybercriminels

Attaquants réputés à un Etat dont Russie et Chine

Qui n'épargne personne

« Pas besoin d'être une cible pour être une victime »

Les vecteurs de compromission



hameçonnage

vulnérabilités logicielles

liens numériques avec ses fournisseurs

LES VECTEURS DE COMPROMISSION

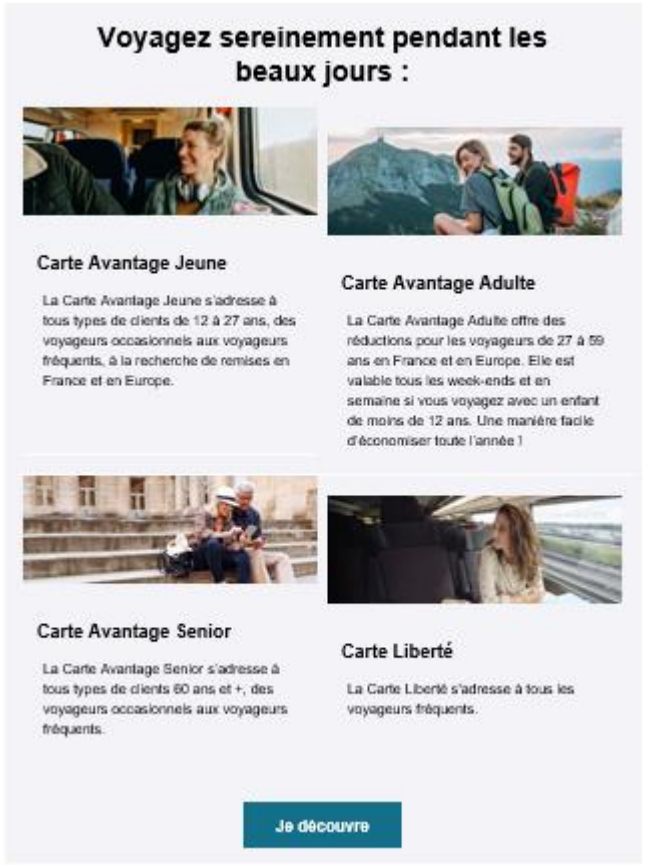
Attaques par hameçonnage (*phishing*)

principes : tenter de récupérer les mots de passe et données personnelles

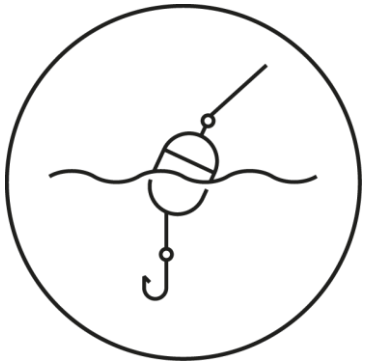
modalités : emails frauduleux, faux sites web

Attention au phishing !

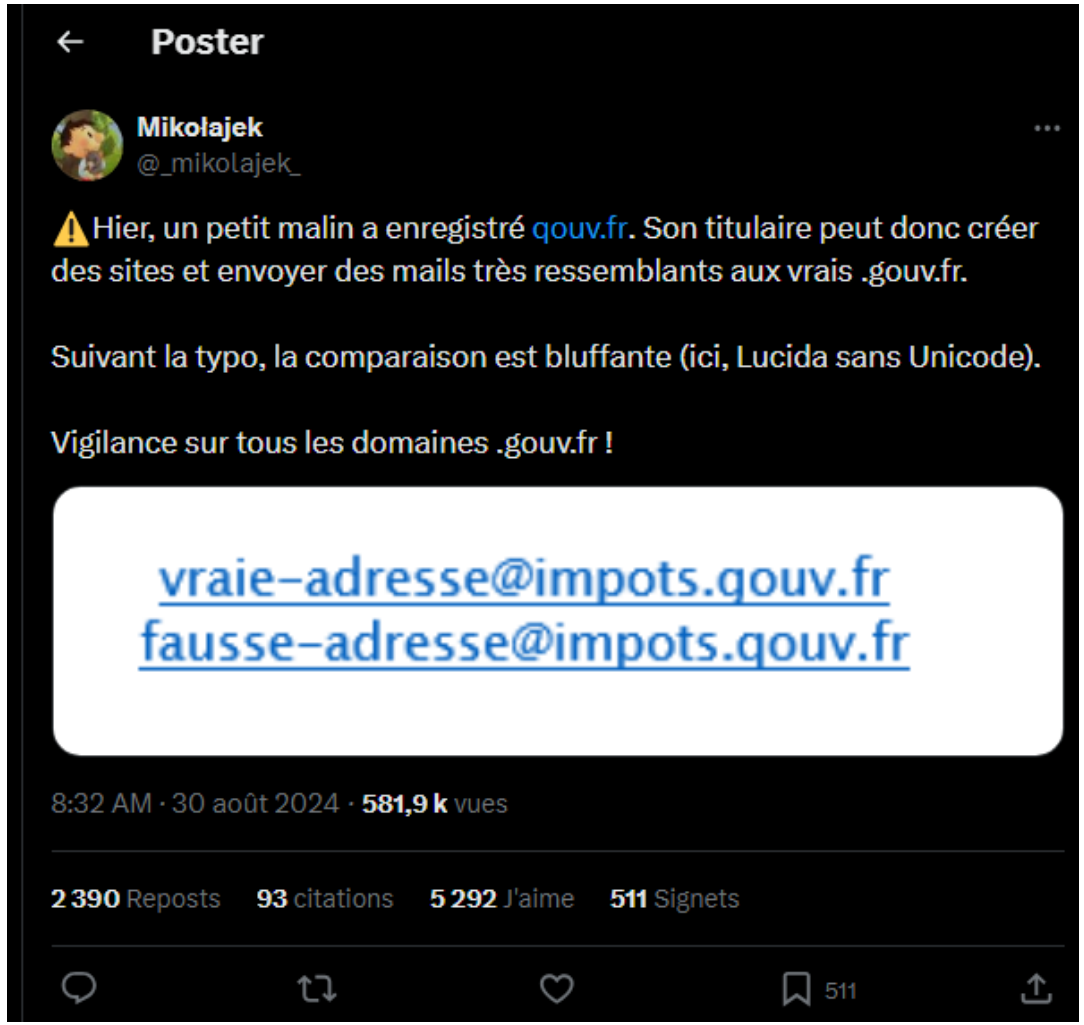
Dans le doute, vérifier l'adresse de l'expéditeur !

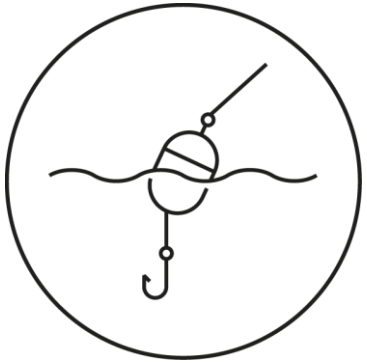


De : **SNCF** <newsletter@promo.livemint.com>
Date: jeu. 17 avr. 2025, 13:43
Subject: Offre limitée : 95% de réduction pendan[illegible]s !
To:



Attention au Typosquatting !

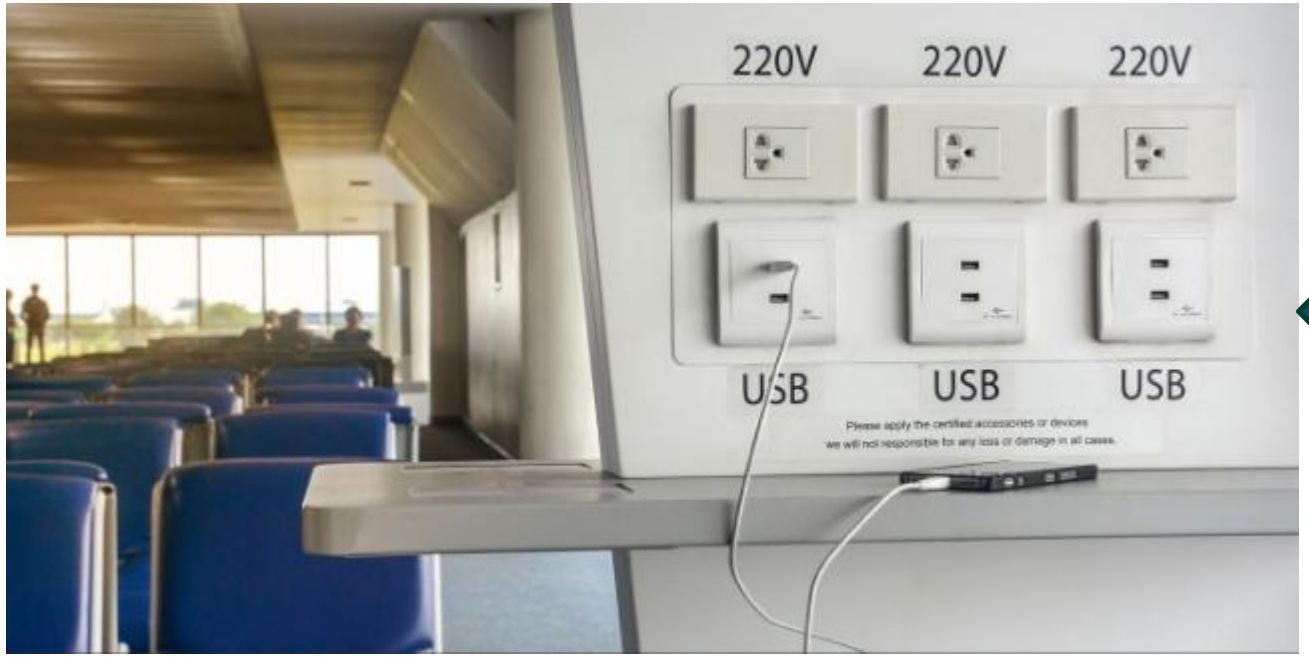




Les variantes : le juice-jacking !

Principe :

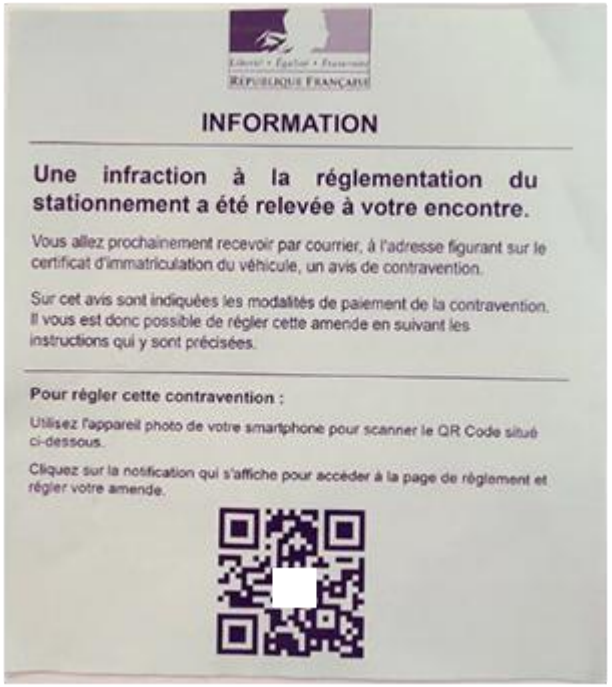
Exfiltrer vos données lorsque vous rechargez votre téléphone dans un lieu public



Les variantes : le quishing !

Principe :

Utiliser un QR code frauduleux pour renvoyer la victime vers un site web malveillant



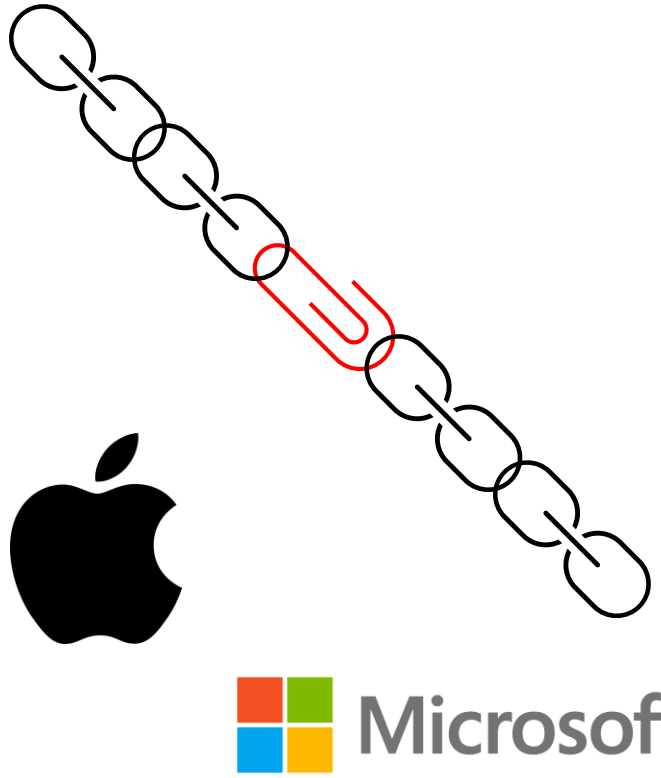
Les faux QR codes peuvent notamment être placés sur les parcmètres et les bornes de recharge pour véhicules électriques. - *Shutterstock /SIPA / SIPA*

LES VECTEURS DE COMPROMISSION

Vulnérabilités logicielles

principes : exploiter les failles logicielles

modalités : exécuter des commandes sensibles avec des outils légitimes ou installer des programmes malveillants

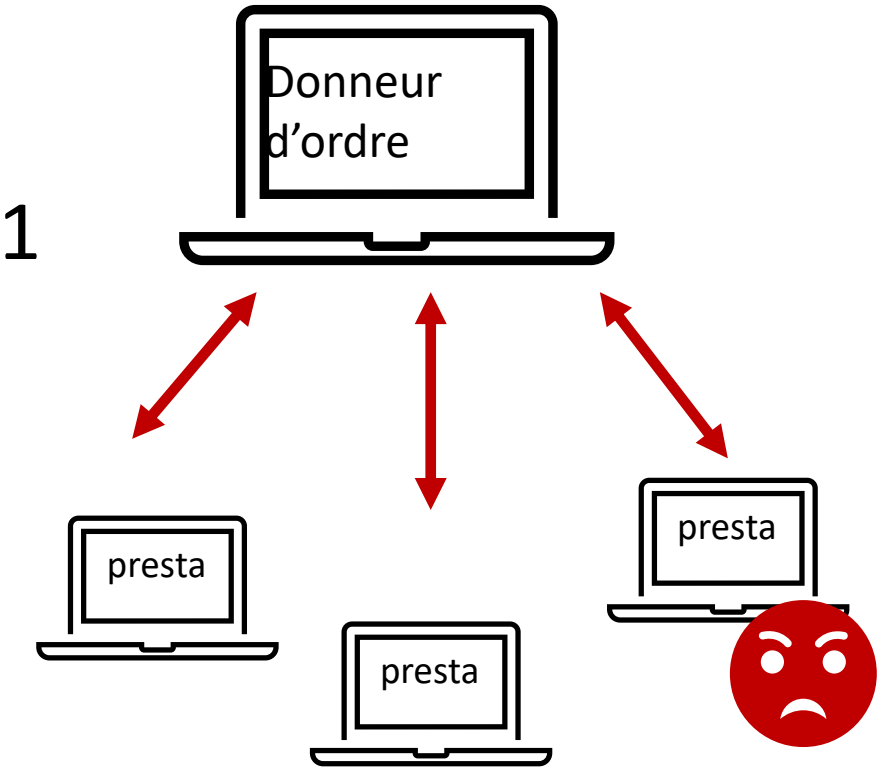


LES VECTEURS DE COMPROMISSION

Les liens numériques avec ses fournisseurs (supply chain)

principes : utiliser des fournisseurs de rang 1 ou 2 pour attaquer le donneur d'ordre

modalités : accès distant, règles d'hygiène faible, utilisation de « moyen perso »

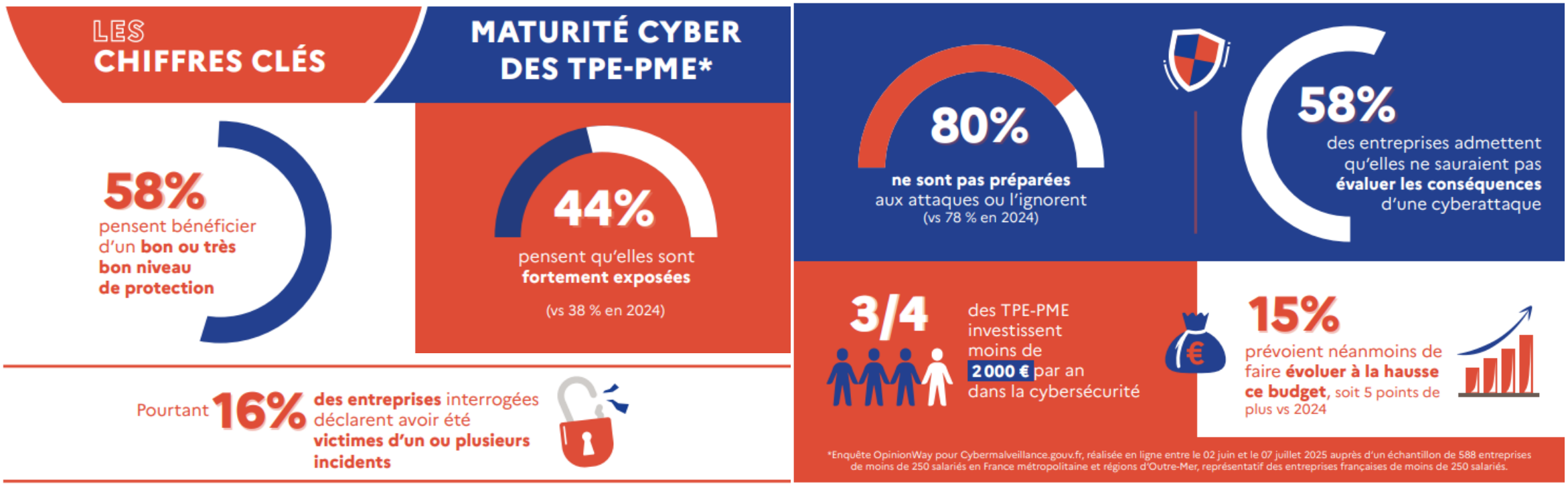


RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

L'ÉTAT DE LA MATURITÉ CYBER

Baromètre national de maturité cyber des TPE-PME – 2e édition

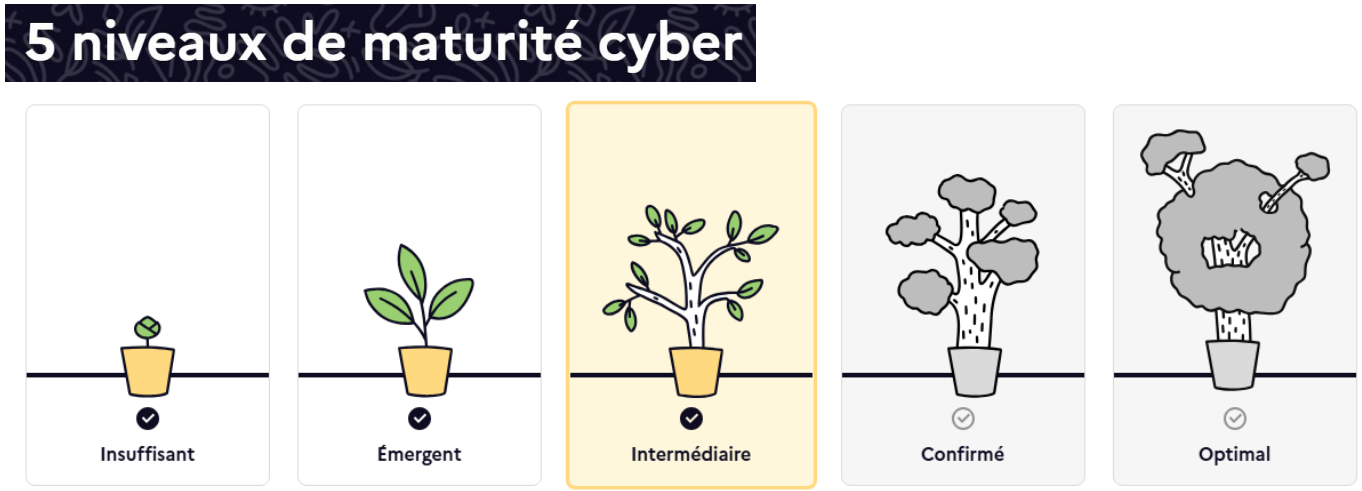
Source : cybermalveillance.gouv.fr – publié le 07/10/2025



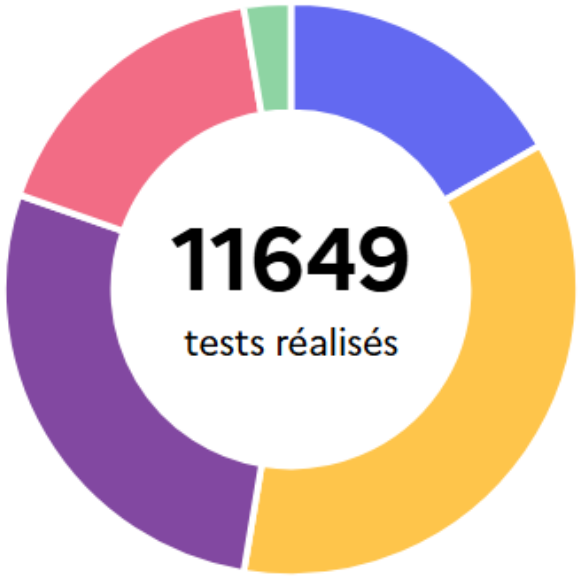
Etat des lieux concernant la maturité cyber

Evaluation de la maturité cyber d'une entité en 7 questions :

https://messervices.cyber.gouv.fr/test-maturite



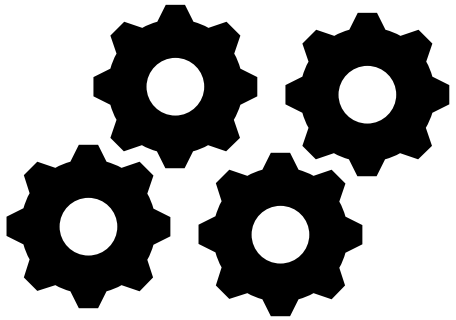
Baromètre de la maturité cyber



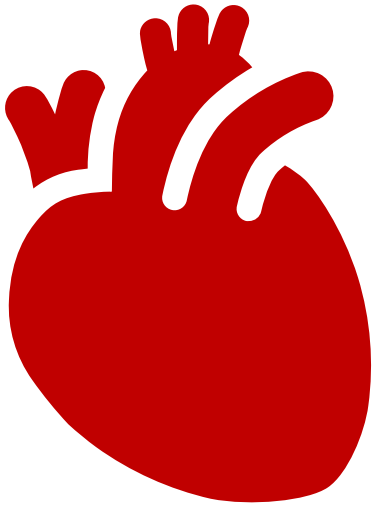
	Tendance nationale France	Tendance région HDF
Insuffisant	**1941** 17%	**97** 15%
Émergent	**4190** 36%	**239** 37%
Intermédiaire	**3226** 28%	**178** 28%
Confirmé	**1984** 17%	**117** 18%
Optimal	**308** 3%	**9** 1%

Source :
Baromètre de la maturité cyber ANSSI
Messervices.cyber.gouv.fr/statistiques (chiffres en date du 22/06/2026)

LE RISQUE CYBER : UN CHANGEMENT DE PARADIGME



Hier
panne informatique = risque technique



Aujourd'hui
cyber attaque = risque stratégique
potentiellement vital

Conséquence législative à venir

la directive européenne
Network and Information System Security

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

NIS 2

Les secteurs concernés

Secteurs hautement critiques

- Santé
- Énergie
- Infrastructures des marchés financiers
- Transports
- Eau potable
- Eaux usées
- Infrastructures numériques
- Administrations publiques
- Secteur bancaire
- Espace
- Gestion des services Technologies de l'Information et de la Communication

Secteurs critiques

- Services postaux et d'expédition
- Industrie manufacturière
- Gestion des déchets
- Recherche
- Fournisseurs numériques
- Fabrication, production et distribution de produits chimiques
- Production, transformation et distribution des denrées alimentaires

Les mécaniques d'identification des entités concernées par la directive NIS 2 seront précisées au travers du processus de transposition de la directive en droit national. L'ANSSI communiquera dès que possible les éléments correspondants.

https://cyber.gouv.fr

PÉRIMÈTRE DES ENTITÉS RÉGULÉES PAR NIS 2

LES SECTEURS DE L'ANNEXE 1

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

LES SECTEURS DE L'ANNEXE 2

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

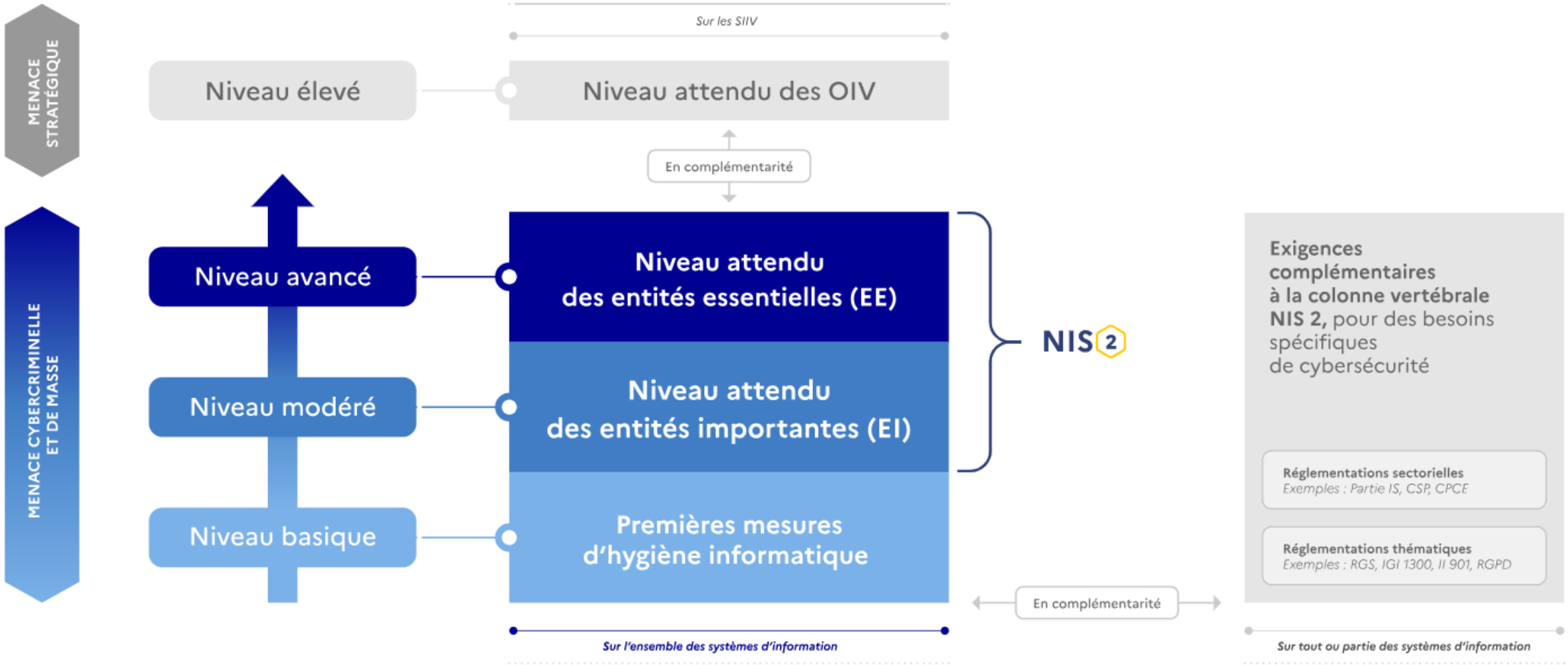
LES ENTITÉS ESSENTIELLES ET IMPORTANTES

SCHÉMATISATION SIMPLIFIÉE DE LA RÈGLE DE BASE

TAILLE ENTITE	NOMBRE D'EMPLOYÉS		CHIFFRE D'AFFAIRES (MILLIONS D'EUROS)		BILAN ANNUEL (MILLIONS D'EUROS)		ANNEXE 1	ANNEXE 2
INTERMÉDIAIRE ET GRANDE	x ≥ 250	**OU**	(y ≥ 50	**ET**	z ≥ 43)		**ENTITES ESSENTIELLES**	**ENTITES IMPORTANTES**
MOYENNE	250 > x ≥ 50	**OU**	(50 > y ≥ 10	**ET**	43 > z ≥ 10)		**ENTITES IMPORTANTES**	**ENTITES IMPORTANTES**
MICRO ET PETITE	x < 50	**ET**	(y < 10	**OU**	z < 10)		***Non concernées***	***Non concernées***

NIS 2 comme colonne vertébrale du cadre règlementaire de cybersécurité

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



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

NIS 2

Un espace dédié aux entités concernées

www.messervices.cyber.gouv.fr/nis2

Les solutions pour aider les organisations publiques et privées à initier leur démarche de sécurisation

Découvrez comment progresser avec MesServicesCyber

La plateforme publique des services et ressources cyber pour aider, proposée par l'ANSSI

Être sensibilisé

Se former

Sécuriser

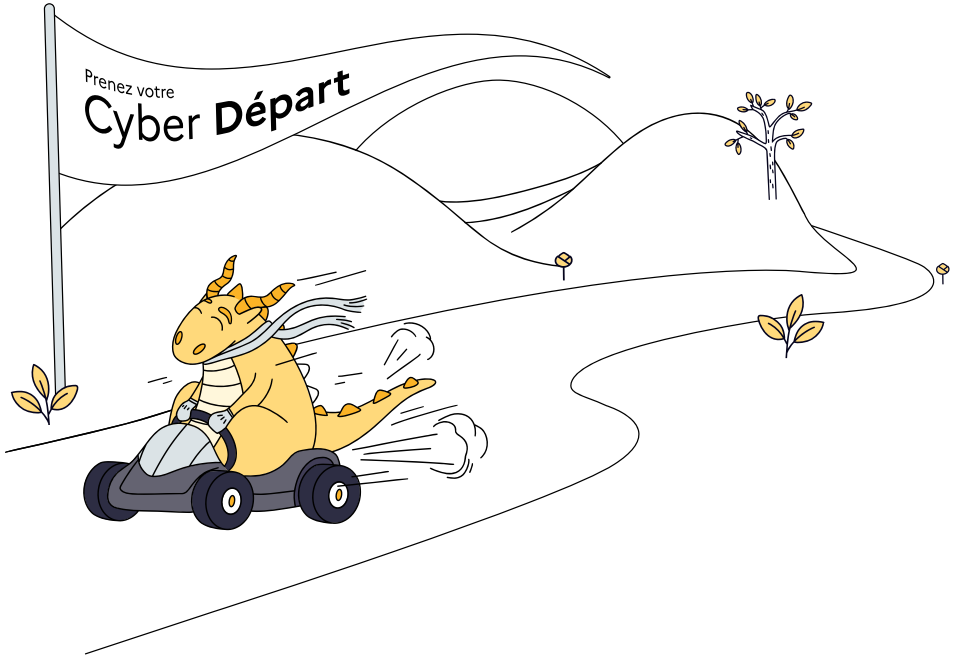
Réagir

Accédez gratuitement à un catalogue complet de services et ressources

https://messervices.cyber.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

Prenez votre Cyberdépart, **en demandant un diagnostic cyber gratuit accompagné par un Aidant cyber**



- Rapide : en 1h30 seulement
- Simple : dans vos locaux ou en visio.
- Utile ! 6 recommandations prioritaires faciles à mettre en œuvre pour se protéger contre les cyberattaques.

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

RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

Merci de votre attention

AGENCE NATIONALE DE LA SECURITE DES SYSTEMES D'INFORMATION

Hugo LONGUESPE

CAMPUS CYBER

HAUTS-DE-FRANCE • LILLE MÉTROPOLE

Le Campus Cyber HDFLM

CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE

Le Campus Cyber Hauts-de-France Lille Métropole fédère les acteurs privés et publics dans le domaine de la cybersécurité.

Il les sensibilise, les guide et les assiste.

Il favorise l'innovation, les compétences et les talents.

Il développe le secteur de la cybersécurité.

Nos 4 missions

CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE

OPÉRER

Renforcer l'autonomie et la capacité des utilisateurs à maîtriser le risque numérique :
- Simuler des attaques avec la CyberRange
- Missions soutenues par le CSIRT Hauts-de-France

MOBILISER

Fédérer les acteurs de la cybersécurité et les entités locales :
- Programmation d'événements
- Animation de groupes de travail

INNOVER

Favoriser l'émergence de nouvelles technologies
3 programmes d'accompagnement :
- Incubation : de l'idée au prototype
- Accélération : croissance et financement des startups
- Alumni : réseautage et business

FORMER

Contribuer à la montée en compétences de l'écosystème :
- Sensibilisation aux risques cyber
- Soutien aux centres de formation

Qui sommes-nous ?

CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE



Le Campus Cyber Hauts-de-France Lille Métropole c'est :

- Le **hub régional** des acteurs de la cybersécurité
- Un réseau de **70 membres** (entreprises, écoles, collectivités, startups, etc.)
- L'un des plus grands **incubateurs de startups cyber** de France
- Un **lieu événementiel** (6 salles de réunion à la location) et un lounge

Notre CyberRange

CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE

Notre Cyber Range, plateforme de simulation de réseaux et d'attaques, propose une gamme complète de services pour renforcer la cybersécurité :

- Des formations spécialisées pour tous les niveaux de compétence
- Formation pratique personnalisée pour simuler des scénarios de la vie réelle
- La gestion de crise pour préparer les équipes à réagir efficacement en cas d'incident
- Simulations avancées pour évaluer et améliorer les défenses contre les menaces

L'équipe

CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE

Chekib GHARBI
Directeur des Opérations

Adrien FATIBENE
Responsable Partenariat
& Développement

Kelly DE BLEECKERE
Responsable Communication
& Evénementiel

Camille DESAUNOIS
Startup Manager & Innovation

Corentin PETRAU
Spécialiste cybersécurité

Mathilde MOUQUET
Chef de projet Marketing Digital

CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE

Nos services

Sensibilisation

CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE

Un module de sensibilisation aux risques cyber, conçu pour faire monter en compétence l'ensemble de vos collaborateurs, quel que soit leur niveau de maîtrise du sujet.
Animée par nos experts, cette session interactive aborde les menaces les plus courantes (phishing, ingénierie sociale, rançongiciels…) et les bons réflexes à adopter au quotidien, à travers des exemples concrets et des mises en situation.

- Durée : 2h
- Public : l'ensemble de vos collaborateurs
- Format : présentiel ou distanciel, gratuit
- Support de sensibilisation remis aux participants à l'issue de la session

Objectif : Adopter les bons réflexes face aux risques cyber au quotidien et réduire le facteur de risque humain au sein de votre structure.

Diagnostic – MonAideCyber

CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE

MonAideCyber
INNOVATION ANSSI

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

MonAideCyber est un dispositif national porté par l'ANSSI.
Il prend la forme d'un audit guidé d'1h30, réalisé par un "aidant de proximité" formé et habilité, directement au sein de votre structure.
L'échange couvre les grands domaines de la cybersécurité : gestion des accès, sauvegardes, mises à jour, sensibilisation des équipes, etc.

- Durée : 1h30
- Dispositif national porté par l'ANSSI
- Réalisé par un aidant formé et habilité
- Restitution sous forme de rapport individuel et confidentiel

Objectif : Obtenir un scoring objectif de sa posture cyber et disposer d'une roadmap priorisée, ainsi que de conseils concrets pour progresser à son rythme.

Tests d'intrusion

CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE

EDIH GREEN POWER IT
PÔLE EUROPÉEN D'INNOVATION NUMÉRIQUE
HAUTS-DE-FRANCE

Une mise à l'épreuve réelle de votre système d'information, réalisée par des experts techniques de notre écosystème, pour identifier les failles avant qu'un attaquant ne les exploite.
Le périmètre (applications, réseau, postes de travail, objets connectés…) est défini avec vous en amont, selon vos enjeux métiers et votre niveau de maturité.

- Durée : à partir de quelques jours, selon le périmètre défini
- Offre jusqu'au 30 juin : 50% du coût pris en charge par l'EDIH
- Restitution détaillée avec niveaux de criticité des vulnérabilités

Objectif : Tester son SI en conditions réelles, remonter les vulnérabilités identifiées et disposer de préconisations de remédiation concrètes et priorisées.

Exercice de gestion de crise

CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE

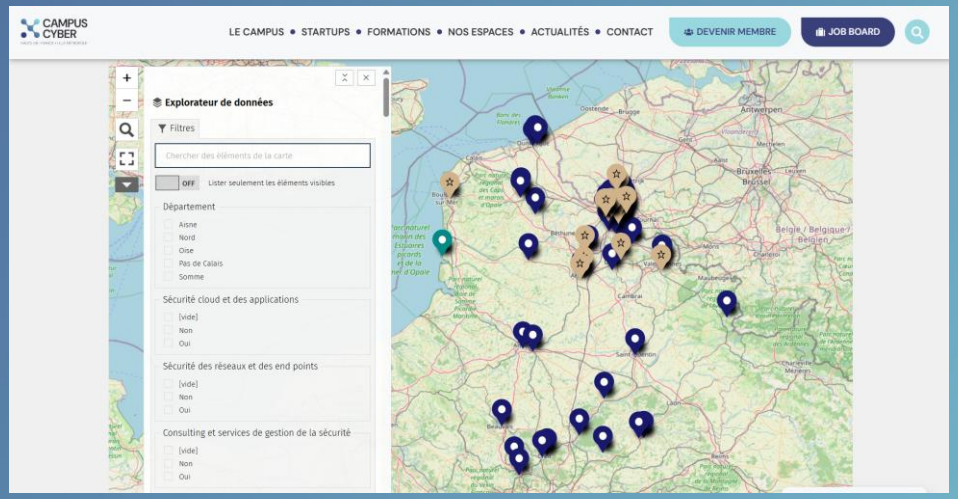
Plongez dans un environnement sous haute tension pour mettre votre organisation à l'épreuve d'une cyberattaque simulée, au plus proche de la réalité.
Cet exercice immersif mobilise vos équipes (direction, IT, communication…) autour d'un scénario réaliste animé par nos experts, qui réagissent en temps réel aux décisions prises.

- Durée : 1/2 journée à 1 journée
- Scénario adapté à votre secteur d'activité
- Débriefing collectif avec axes d'amélioration à l'issue de l'exercice

Objectif : Forger les premiers réflexes cyber, fluidifier la coordination entre équipes et gagner en efficience sur vos process de gestion de crise.

Cartographie des acteurs cyber

CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE



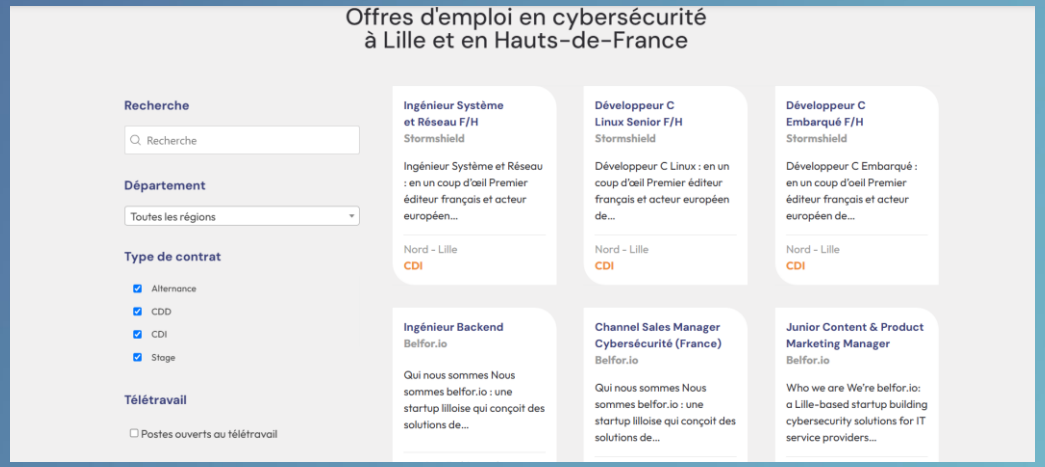
Une cartographie en ligne, mise à jour régulièrement, qui recense plus de 150 acteurs cyber de la région Hauts-de-France : entreprises, prestataires, écoles, laboratoires et organismes publics.
Les acteurs sont classés par domaine d'expertise (sécurité cloud, sécurité réseau, services et conseil, sécurité des données, formation) pour vous orienter rapidement vers le bon interlocuteur, en fonction de votre besoin.

- Disponible gratuitement sur hdf.campuscyber.fr (onglet cartographie)
- Plus de 150 acteurs régionaux référencés
- Fiches détaillées par acteur (services, coordonnées, zone d'intervention)

Objectif : Savoir qui contacter pour quel besoin, et identifier rapidement un prestataire de confiance de proximité.

Job Board

CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE



Une bourse à l'emploi dédiée aux métiers de la cybersécurité, pensée pour faciliter la mise en relation entre vos besoins de recrutement et les talents de la région.
Vos offres sont relayées directement auprès des écoles et organismes de formation partenaires du Campus Cyber, sur l'ensemble des Hauts-de-France.

- Diffusion auprès des écoles et centres de formation de la région
- Visibilité auprès d'un vivier de profils en formation ou en alternance
- Service proposé sans surcoût pour les membres du Campus Cyber

Objectif : Recruter vos profils cyber et faciliter votre accès aux talents de demain.

Solutions innovantes

CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE

Plusieurs solutions innovantes, souveraines et locales pour équiper votre structure, directement issues des startups accompagnées par notre incubateur.
Du SaaS de gestion des vulnérabilités à la protection des identités numériques, ces solutions couvrent un large spectre de besoins cyber, avec un accompagnement de proximité assuré par les équipes fondatrices.

- Solutions développées et hébergées en France
- Plusieurs solutions disponibles en modèle open-source (gratuit)
- Mise en relation directe avec les startups pour un accompagnement personnalisé

Objectif : Vous équiper avec des solutions locales, souveraines et adaptées à vos besoins, tout en soutenant l'écosystème cyber régional.

OpenCVE

ADES

Campus Cyber Summit

CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE

Un événement annuel incontournable qui réunit l'ensemble de l'écosystème cyber régional autour de conférences, tables rondes et retours d'expérience.
Experts, entreprises, institutions et chercheurs partagent leur regard sur l'actualité cyber, dans un format pensé pour favoriser les échanges et le réseautage entre participants.

- Thématiques abordées : retour d'expérience suite à une attaque, NIS 2, assurances cyber…
- Conférences, tables rondes et temps de networking
- Ouvert à l'ensemble de l'écosystème : entreprises, collectivités, écoles

Objectif : Partager les bonnes pratiques, monter en compétence collectivement et rester à jour face aux nouvelles menaces.

CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE

Bâtiment Wenov
177 allée Clémentine Deman
59000 Lille

campus@hdf.campuscyber.fr
hdf.campuscyber.fr


CSIRT
HAUTS-DE-FRANCE

CSIRT HAUTS-DE-FRANCE

4 missions de service public, gratuites pour les bénéficiaires

1. Réponse aux incidents cyber
2. Mise en relation avec des prestataires qualifiés
3. Facilitation des relations avec les partenaires publics
4. Assistance et conseil sur l'évaluation des risques et la conformité

CSIRT HAUTS-DE-FRANCE

Risque juridique : responsabilité contractuelle, sanctions en cas d'irrégularités …

Risque financier : amendes, dépenses imprévues, fragilisation de la stabilité financière …

Risque réputationnel : perte de confiance des clients, partenaires et parties prenantes …

Risque de sécurité : vol de données, fuite de technologies, cyberattaques …

CSIRT HAUTS-DE-FRANCE

2 moyens de contact

- Web : **csirt-hdf.fr**

- Téléphone : **0806 700 111**

CSIRT
HAUTS-DE-FRANCE

EN CAS DE CYBERATTAQUE APPELEZ LE :

0806 700 111

CSIRT HAUTS-DE-FRANCE

Soutenu par

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Région Hauts-de-France

CITC DIGITAL INNOVATION HUB HAUTS-DE-FRANCE

EDIH GREEN POWER IT
EUROPEAN DIGITAL INNOVATION HUB HAUTS-DE-FRANCE

Cofinancé par l'Union européenne

La Région Hauts-de-France s'engage en faveur de la Cybersécurité

Programme

1. Présentation des structures et correspondants

2. Présentation de la thématique : Enjeux de Cybersécurité pour les entreprises de la filière Energie

3. Questions / Réponses

4. Prochain webinaire

Programme

1. Présentation des structures et correspondants

2. Présentation de la thématique : Enjeux de Cybersécurité pour les entreprises de la filière Energie

3. Questions / Réponses

4. Prochain webinaire

Prochain webinaire programmé avec

Interlocuteurs privilégiés : Direction + Resp. QHSE + Resp. Dvpt. Commercial

	Titres	Animations	Dates	Horaires
N°7	**EPR2 Emploi & Compétences**	Anne-Laure LAFAYE – Resp. EPR2 Emploi & Compétences (FRANCE TRAVAIL) Elyne VOLTA – Chargé de mission intégration territoriale EPR2 (EDF)	02/07/2026	8h-9h

MERCI pour votre attention et à bientôt !

MEDEE

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ANSSI

CAMPUS CYBER
HAUTS-DE-FRANCE • LILLE MÉTROPOLE

DGSI

NUCLÉI
Hauts-de-France