CAMPUS CYBER

HAUTS-DE-FRANCE • LILLE MÉTROPOLE

Kit Conseil Cybersécurité

PME & COLLECTIVITÉS

MARS 2024

FRANCE 2030

UNION EUROPÉENNE

l'Europe s'engage en Hauts-de-France avec le FEDER

Région Hauts-de-France

MEL MÉTROPOLE EUROPÉENNE DE LILLE

EURATECHNOLOGIES EUROPE'S STARTUP BUILDER

INTRODUCTION

Ce kit conseil réalisé par le Campus Cyber Hauts-de-France Lille Métropole a pour objectif d'aider les collectivités et les entreprises qui souhaitent s'informer sur les risques cyber, veulent connaitre les mesures indispensables à mettre en place et ont besoin de savoir à qui s'adresser quand elles sont victimes d'une cyber attaque. Le livret s'appuie sur les documents proposés gratuitement par les organismes et institutions publiques (ANSSI, Cybermalveillance.gouv.fr, Gendarmerie Nationale, Police Nationale, CNIL...) et n'a pas vocation d'exhaustivité. Il s'inscrit dans les missions du Campus Cyber Hauts-de-France Lille Métropole d'œuvrer à la sensibilisation et à la protection cyber des acteurs économiques du territoire.

C'est pourquoi, nous proposons également un volet particulièrement destiné aux organisations publiques et privées des Hauts-de-France.




À propos du Campus Cyber Hauts-de-France Lille Métropole

Le Campus Cyber Hauts-de-France Lille Métropole fédère acteurs privés et publics sur les enjeux de cybersécurité. Il les sensibilise, les oriente et les assiste. Il fait émerger l'innovation, les compétences et les talents. Il développe la filière économique cyber.

campus@hdf.campuscyber.fr

hdf.campuscyber.fr

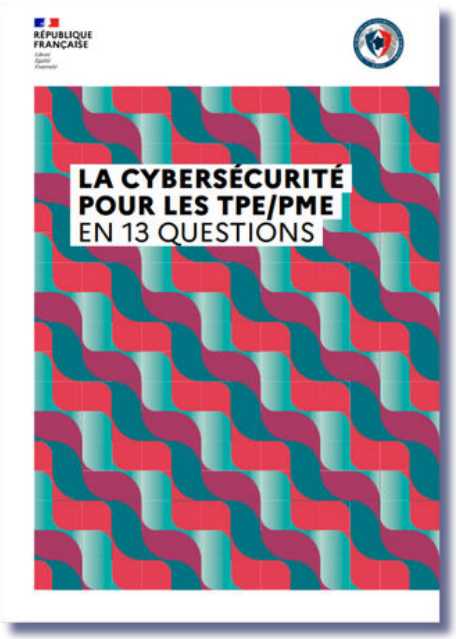
L'AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (ANSSI)

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) est l'autorité nationale en matière de cybersécurité. Sa mission est de comprendre, prévenir et répondre au risque cyber.

Son action pour la protection de la Nation face aux cyberattaques se traduit en quatre grandes missions : défendre, connaître, partager, accompagner. Dans ce cadre, l'ANSSI propose un ensemble de ressources (guides, bonnes pratiques…) pour informer les entreprises et les collectivités et les aider à se protéger.

cyber.gouv.fr

RESSOURCES UTILES



Ce guide présente, en treize questions, des mesures accessibles pour une protection globale de l'entreprise.

En mettant en place des mesures simples mais essentielles, vous pourrez protéger votre entreprise contre de nombreuses cybermenaces et considérablement limiter les dégâts en cas d'attaque de haut niveau.

cyber.gouv.fr/publications/la-cybersecurite-pour-les-tpepme-en-treize-questions

CYBERMALVEILLANCE.GOUV.FR

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

Cybermalveillance.gouv.fr a pour missions d'assister les particuliers, les entreprises, les associations, les collectivités et les administrations victimes de cybermalveillance, de les informer sur les menaces numériques et les moyens de s'en protéger.

www.cybermalveillance.gouv.fr

RESSOURCES UTILES

13 fiches à retrouver* pour les entreprises et les collectivités :

- Piratage d'un système informatique professionnel, que faire ?
- Virus informatique, que faire ?
- FOVI ou arnaque au faux ordre de virement bancaire, que faire ?
- Fraude à la carte bancaire, que faire ?
- Défiguration de site Internet, que faire ?
- Que faire en cas de phishing ou hameçonnage ?
- Rançongiciel ou ransomware, que faire ?
- Spam téléphonique, que faire ?
- Spam électronique, que faire ?
- Piratage de compte, que faire ?
- Comment faire face à l'arnaque au faux support technique ?
- Attaque DDoS, que faire ?
- Que faire en cas de piratage de son espace recruteur sur un site d'emploi ?

** disponibles également en annexes*

PME/TPE COLLECTIVITÉS À QUI S'ADRESSER ?

S'INFORMER & PRÉVENIR

POUR S'INFORMER

- **Cybermalveillance.gouv.fr :** www.cybermalveillance.gouv.fr
- **ANSSI Hauts-de-France :** hauts-de-france@ssi.gouv.fr
- **Gendarmerie Nationale :** www.gendarmerie.interieur.gouv.fr/conseils/numerique
- **Préfecture de Police :** www.prefecturedepolice.interieur.gouv.fr/prevention/nos-conseils/cybersecurite
- **Campus Cyber Hauts-de France Lille Métropole :** hdf.campuscyber.fr
- **CNIL :** www.cnil.fr/fr/professionnel

POUR BÉNÉFICIER D'UNE SENSIBILISATION GRATUITE

- **ANSSI Hauts-de-France :** hauts-de-france@ssi.gouv.fr
- **Campus Cyber Hauts-de France Lille Métropole :** hdf.campuscyber.fr
- **CSIRT Hauts-de-France :** csirt-hdf.fr
- **Tuto de cybermalveillance.gouv.fr pour les collectivités territoriales :** www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/programme-sensibilisation-risques-numeriques-collectivites-territoriales
- **Gendarmerie Nationale** : 03 20 43 57 56 / securite-economique-hauts-de-france@gendarmerie.interieur.gouv.fr

POUR BÉNÉFICIER D'UN DIAGNOSTIC GRATUIT

L'ANSSI propose **MonAideCyber**, un service gratuit de diagnostic cyber rapide, réalisé par des tiers de confiance, formés, outillés par l'ANSSI, rassemblés au sein d'une communauté. MonAideCyber s'adresse aux entités publiques et privées - quelle que soit leur taille - déjà sensibilisées au risque et souhaitant s'engager dans une démarche adaptée et concrète de renforcement de leur cybersécurité. Localement, plusieurs référents peuvent vous accompagner dans la démarche dont le Campus Cyber Hauts-de-France Lille Métropole (hdf.campuscyber.fr).

RÉAGIR EN CAS D'ATTAQUE

EN CAS D'ACTE DE CYBER MALVEILLANCE

- **CSIRT Hauts-de-France : 0 806 700 111** (csirt-hdf.fr)
- **Police - Gendarmerie : 17** (Pour les personnes sourdes et malentendantes, envoyez un SMS au 114)
- **Cybermalveillance.gouv.fr :** www.cybermalveillance.gouv.fr/diagnostic/profil
- **ANSSI**, pour les entités régulées et certaines administrations : cyber.gouv.fr/en-cas-dincident
- **CNIL**, pour déposer une plainte relative à vos données personnelles : www.cnil.fr/fr/plaintes

EN CAS DE FRAUDE À LA CARTE BANCAIRE

La plateforme **Percev@l** vise à lutter contre la fraude à la carte bancaire sur Internet. Elle permet à tout internaute de signaler aux forces de l'ordre un ou plusieurs usages frauduleux de sa carte bancaire :
www.service-public.fr/particuliers/vosdroits/R46526

POUR SIGNALER DES CONTENUS ILLICITES

La Plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (**Pharos**) du ministère de l'Intérieur procède prioritairement au traitement des signalements de contenus illicites mis en ligne. Arnaques, discriminations, menaces d'atteintes aux personnes, faits liés au terrorisme, urgences vitales, pédopornographie, peuvent notamment être portées à la connaissance des autorités grâce à ce dispositif. Pharos initie des enquêtes judiciaires chaque fois que nécessaire :
www.internet-signalement.gouv.fr/PharosS1/

LUTTER CONTRE LES SPAMS VOCAUX ET SMS

Le service **33700**, plateforme de lutte contre les spams vocaux et SMS, vous informe et vous accompagne : www.33700.fr

EN CAS D'ESCROQUERIE EN LIGNE

La plateforme **Thésée** permet aux victimes d'e-escroqueries de déposer plainte en ligne facilement et rapidement. L'accès à Thésée se fait à partir de la rubrique « Arnaque sur Internet » du site service-public.fr : www.service-public.fr/particuliers/vosdroits/N31138.

TROUVER UN FINANCEMENT

FRANCE 2030 – DIAGNOSTIC CYBERSÉCURITÉ

Objet : renforcer la cybersécurité des entreprises

Opérations éligibles :
Mission de conseil sur 8 jours ayant pour objectif de :

- **sensibiliser** le comité de direction et diffuser les bonnes pratiques en matière de cybersécurité ;
- effectuer **un bilan des forces et des faiblesses** de la protection de votre SI ;
- proposer des **recommandations priorisées, chiffrées et adaptée**s au contexte de votre entreprise afin d'assurer un niveau de sécurité adéquat,
- préparer l'entreprise à la **gestion de crise cyber**.

Bénéficiaires :
PME indépendantes. Les ETI peuvent être éligibles en fonction du périmètre d'intervention concerné, sous réserve de l'accord de Bpifrance.

Montant :
Subvention représentant **50 % des dépenses éligibles**, pour un coût total du diagnostic de **8 800€ HT**. Le reste à charge pour l'entreprise est de **4 400 €**.

Sources : Hexatrust

FRANCE 2030 – CYBER PME

Objet : accompagner les PME et ETI qui souhaitent renforcer leur niveau de sécurité et se protéger des risques.

Opérations éligibles :

- Réalisation d'un **diagnostic Cybersécurité** : 8 jours homme répartis sur une durée de 3 à 5 mois maximum ;
- **Mise en œuvre des recommandations** du diagnostic : plan de financement pouvant s'étendre sur une durée de 12 à 18 mois.

Bénéficiaires :

PME et ETI de tous secteurs d'activité.
Une priorité est donnée aux entreprises dont l'activité s'inscrit dans les secteurs de l'aéronautique civile et de l'énergie au sens de la directive européenne NIS2.

Montant :

- **Diagnostic Cybersécurité** : diagnostic d'un coût de **8 800 € HT subventionné à 50 %** soit 4 400 € HT de reste à charge pour l'entreprise ;
- **Subvention** allant de **30 000 à 80 000 €** pour financer jusqu'à 70 % des dépenses liés au plan de sécurisation remis en fin de diagnostic.

Sources : Hexatrust

MISSION DE CONSEIL CYBERSÉCURITÉ

Objet : réaliser un état des lieux de votre situation, établir un plan de sécurisation de vos symptômes informatiques et de sensibiliser vos collaborateurs aux meilleures pratiques d'usage du SI.

Opérations éligibles :

13 jours homme d'intervention sur 6 à 8 semaines, pour :

- des entretiens individuels (internes et externes), une visite des installations et une revue documentaire,
- un diagnostic flash « Sécurité SI » sur 10 axes,
- 1 à 2 séances de sensibilisation en présentiel à destination des utilisateurs,
- des entretiens ou ateliers complémentaires avec les sachants techniques pour mettre au point le plan d'action et définir les priorités,
- une présentation des travaux à l'équipe dirigeante

Bénéficiaires :

PME réalisant un CA minimum de 12 M €
Ayant au minimum 3 ans d'existence et 10 salariés
et ETI

Montant :

Reste à charge clients Bpifrance : 9 000€ HT.

Sources : Hexatrust

TROUVER UN FINANCEMENT EN HAUTS-DE-FRANCE

PASS CYBER FORMATION

Objet : permettre aux TPE ou PME de renforcer leurs compétences sur les enjeux et conséquences d'une menace cyber.

Opérations éligibles :

Réalisation d'un diagnostic de cybersécurité d'une durée de 10 jours et d'un coût de 10 000 € HT.

Bénéficiaires :

TPE et PME

Montant :

Prise en charge de la région à hauteur de 50 % du coût estimé pour l'entreprise (dans la limite de 200 € HT par journée de formation).

PASS CYBER CONSEIL

Objet : accompagner les entreprises au déploiement d'une organisation efficiente en matière de sécurité informatique via des audits ou études techniques d'évaluation et de préconisations.

Opérations éligibles :

- Audit sécurité informatique (analyse globale du SI de l'entreprise) ;
- Audit d'architecture (réseau et infrastructure), audit système d'exploitation, audit organisationnel ;
- Tests de sécurité web ;
- Tests d'intrusion interne du réseau de l'entreprise ;
- Tests d'intrusion externe ;
- Analyse « forensic » post-intrusion ;
- Accompagnement à la mise en place d'une politique de sécurité informatique.

Bénéficiaires :

TPE et PME

Montant :

Subvention représentant 50 % des prestations, dans la limite de 10 000 € par prestation.

Sources : Hexatrust

PASS CYBER INVESTISSEMENT

Objet : Accompagner les entreprises s'engageant dans un plan d'investissement en matière de Cybersécurité (investissements matériels et incorporels).

Opérations éligibles :

- Mesures de protection réseau ;
- Solutions de cyber veille (Cyber Threat Intelligence) pour détecter, investiguer et traquer des menaces inconnues et émergentes : plateforme de veille de cybersécurité / logiciel de gestion des risques opérationnels ;
- Evolution technologique de l'environnement informatique OU Mises à jour logicielles et systèmes.

Bénéficiaires :

PME

Montant :

Subvention représentant 30 % des dépenses éligibles, comprise entre 900 et 4500 €.

Sources : Hexatrust

ANNEXES

CAMPUS CYBER

HAUTS-DE-FRANCE • LILLE MÉTROPOLE

Bâtiment WENOV
177 allée Clémentine Deman
59000 Lille

campus@hdf.campuscyber.fr

hdf.campuscyber.fr

FRANCE 2030
UNION EUROPÉENNE
l'Europe s'engage en Hauts-de-France avec le FEDER
Région Hauts-de-France
MEL MÉTROPOLE EUROPÉENNE DE LILLE
EURATECHNOLOGIES EUROPE'S STARTUP BUILDER