Risques majeurs et menaces cyber : se préparer à des crises combinées

AFPCNT
Association Française pour la Prévention des Catastrophes Naturelles et Technologiques
Mieux comprendre, mieux prévenir

Soutenu par
MINISTÈRE DE LA TRANSITION ÉCOLOGIQUE ET DE LA COHÉSION DES TERRITOIRES
Liberté
Égalité
Fraternité

RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

Comprendre les risques de Cybersécurité
AFPCNT

AGENCE NATIONALE DE LA SECURITE DES SYSTEMES D'INFORMATION

Martin Véron

Présentation de l'ANSSI

Rattachement

Services du Premier Ministre

SGDSN
Secrétariat Général de la Défense et de la Sécurité Nationale

Coordination interministérielle en matière de défense et de sécurité nationale

ANSSI
Agence Nationale de Sécurité des Systèmes d'Information

Autorité nationale en matière de sécurité et de défense des systèmes d'information

Créée le 7 juillet 2009 par le décret n°2009-934, l'ANSSI est un **service à compétence nationale.**

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Bénéficiaires prioritaires

Opérateurs d'importance vitale | Opérateurs de services essentiels | Administrations et opérateurs publics

Défendre

CERT-FR Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques

Supervisions de
certains SI critiques

Traitement des incidents ou
soutiens auprès des victimes (État, OIV, OSE)

Veille sur les
vulnérabilités et incidents

...

Connaître

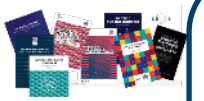
Évaluer en continu les menaces
et les risques dans le cyberespace

Développer des méthodes
et des outils pour y faire face

Expertise, labos de recherche,
veille technologique

...

Partager



SecNumacadémie.gouv.fr
Formez-vous à la sécurité du numérique

SecNumedu
ANSSI

Aider à faire prendre conscience
des risques numériques d'aujourd'hui

Guides, MOOC,
notes techniques et méthodologiques

Centre de formation SSI
et labellisation de formations

...

Accompagner

VISA DE SÉCURITÉ

Appuyer le gouvernement dans le
déploiement d'une politique publique cyber

Aider au développement d'un écosystème de
prestataires et de produits/services de confiance

Agir aux échelons
européen, national et territorial

...

Etat de la menace cyber

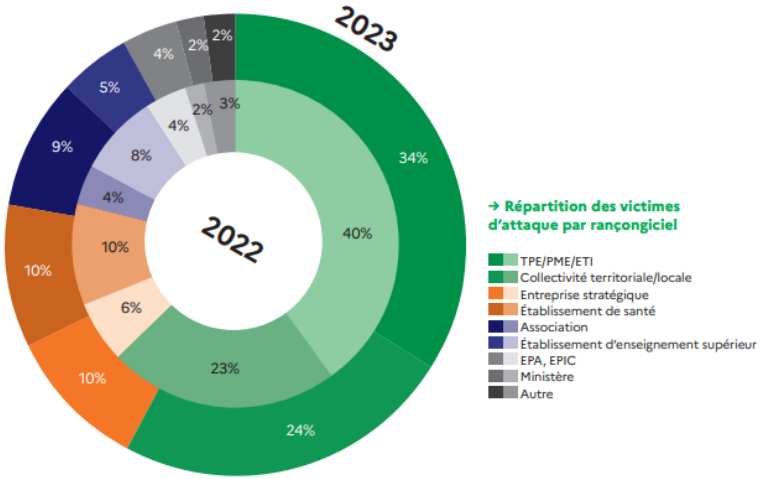
Le risque numéro 1, en évolution croissante

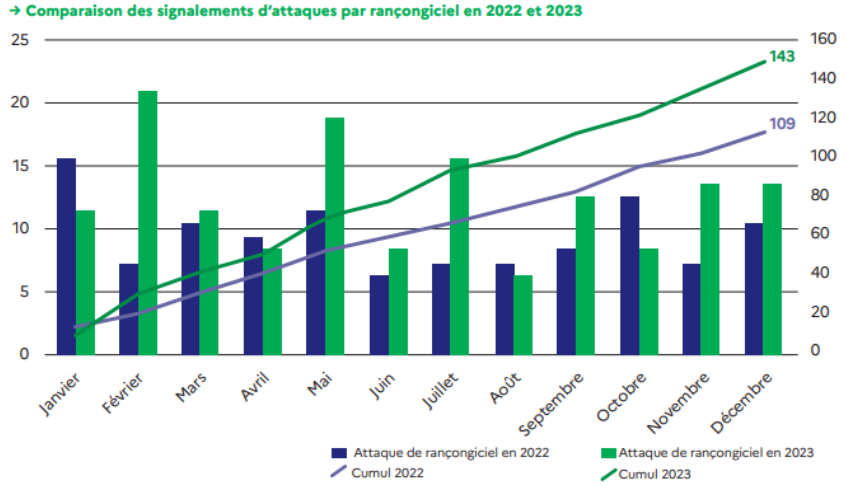
> En 2020 nombre d'incidents cyber traités **multiplié par 4 ;** en 2021, **augmentation de 40% ; légère baisse** en début 2022 ; **réhausse en 2023**

> Principales motivations : appât du gain (extorsion, rançon, revente de données, escroquerie), déstabilisation et sabotage

> Professionnalisation des hackers, **développement d'attaques automatisées via l'IA**, phénomène de « pèche au chalut »

> Une menace qui s'adapte à l'actualité : **Jeux Olympiques Paris 2024**

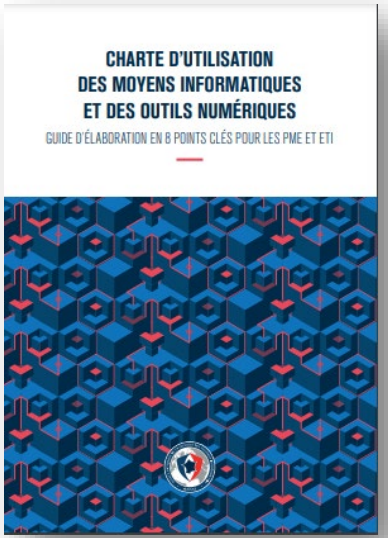




Conseils et recommandations

Responsabiliser vos collaborateurs, votre 1er maillon de cybersécurité

Sensibilisation régulière des utilisateurs, des décideurs et des partenaires



Conseils et recommandations

Faites un 1er diagnostic pour connaitre ses lacunes et les corriger via une approche adaptée

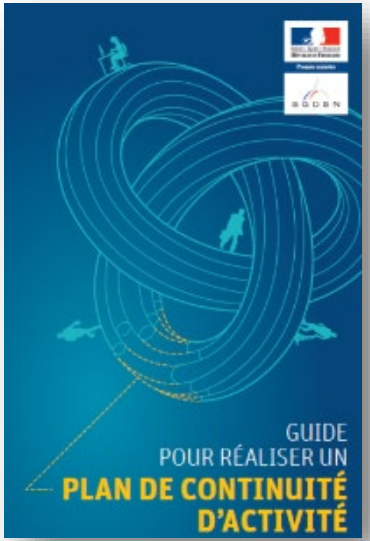
MonAideCyber
INNOVATION ANSSI

monaidecyber@ssi.gouv.fr

Conseils et recommandations

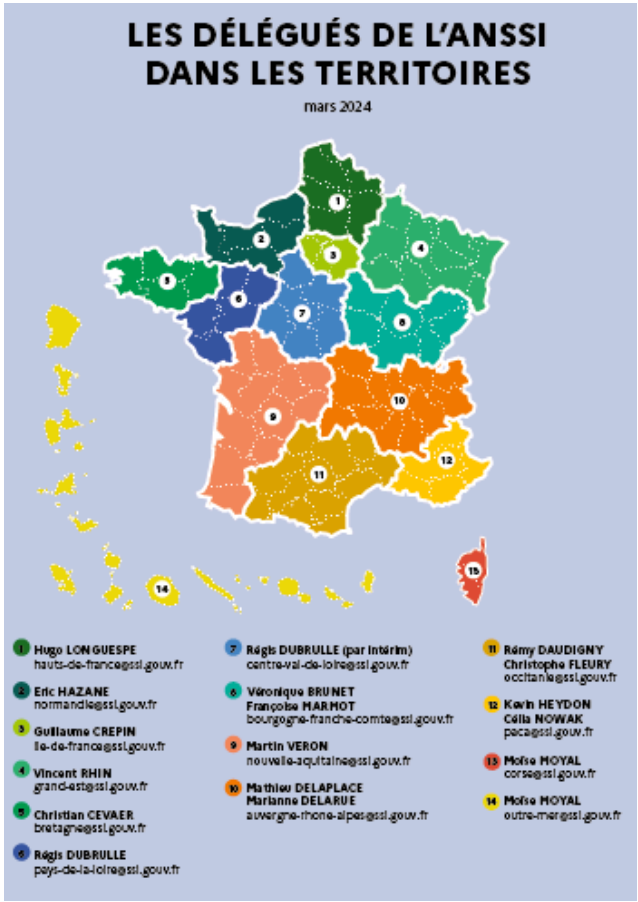
Anticiper une crise d'origine cyber

Développer des réflexes et des modes dégradés : quoi faire, qui contacter, quelles sont nos priorités ?



Contacts territoriaux

Région	Numéro Vert
Bourgogne-Franche-Comté	0 970 609 909
Bretagne	0 800 200 008
Centre-Val de Loire	0 805 69 15 05
Grand Est	0 970 512 525
Hauts-de-France	0 806 700 111
Île-de-France	0 800 730 647
Normandie	0 808 800 001
Nouvelle-Aquitaine	0 805 29 29 40
Occitanie	0 800 71 13 13
Pays de la Loire	0800 100 200
Provence-Alpes-Côte d'Azur	0 805 036 083



RÉGION
Nouvelle-
Aquitaine

C3 CAMPUS RÉGIONAL DE CYBERSÉCURITÉ ET DE CONFIANCE NUMÉRIQUE
Nouvelle-Aquitaine

Le Projet de la région Nouvelle Aquitaine

OPERATION (CSIRT)
Réponse à incidents

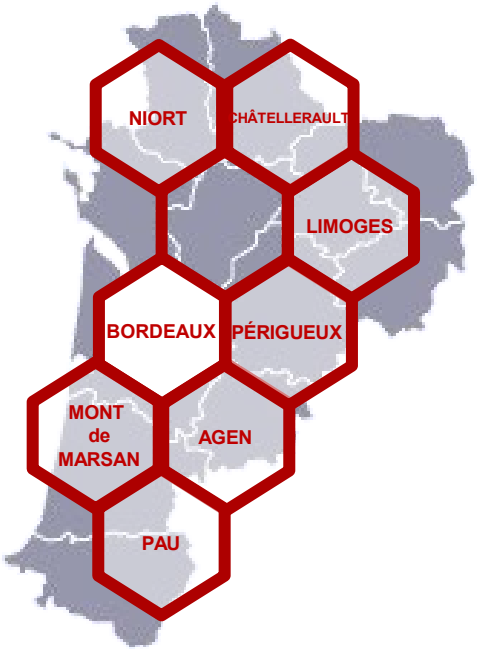
INNOVATION
Accompagnement de projets innovants

FORMATION
Organisation de sessions de formations
(ex: parcours Expert Cyber, …)

ANIMATION
Mise en réseau des acteurs à l'échelle d'un territoire
Actions d'animation d'écosystème

SENSIBILISATION
Actions de sensibilisation aux enjeux de la cybersécurité

ACCOMPAGNEMENT
(ex : accès à des ressources techniques et humaines, mise en place de marchés cadres pour l'acquisition de solutions de cybersécurité, …)



Un conseil d'administration qui s'étoffe

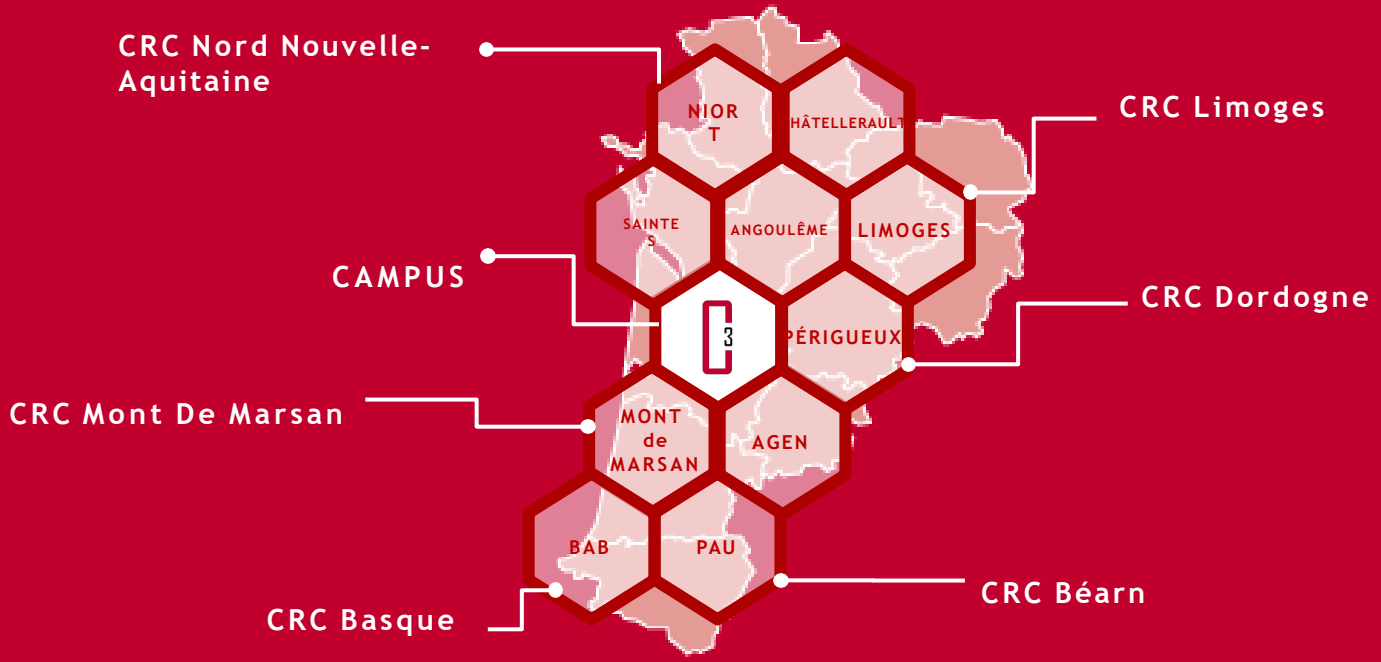
MEMBRES FONDATEURS

MEMBRES ASSOCIÉS

MEMBRES ÉLUS

- Entreprises
- Formation
- Ordres professionnels
- Institutionnel
- Association / Clusters
- Partenaires

Une couverture régionale



Un centre de réponse à incidents

- Opération

Anticipation

Diagnostic

Détection

Réponse à incident

CRIC CENTRE DE RÉPONSE AUX INCIDENTS CYBER Nouvelle-Aquitaine

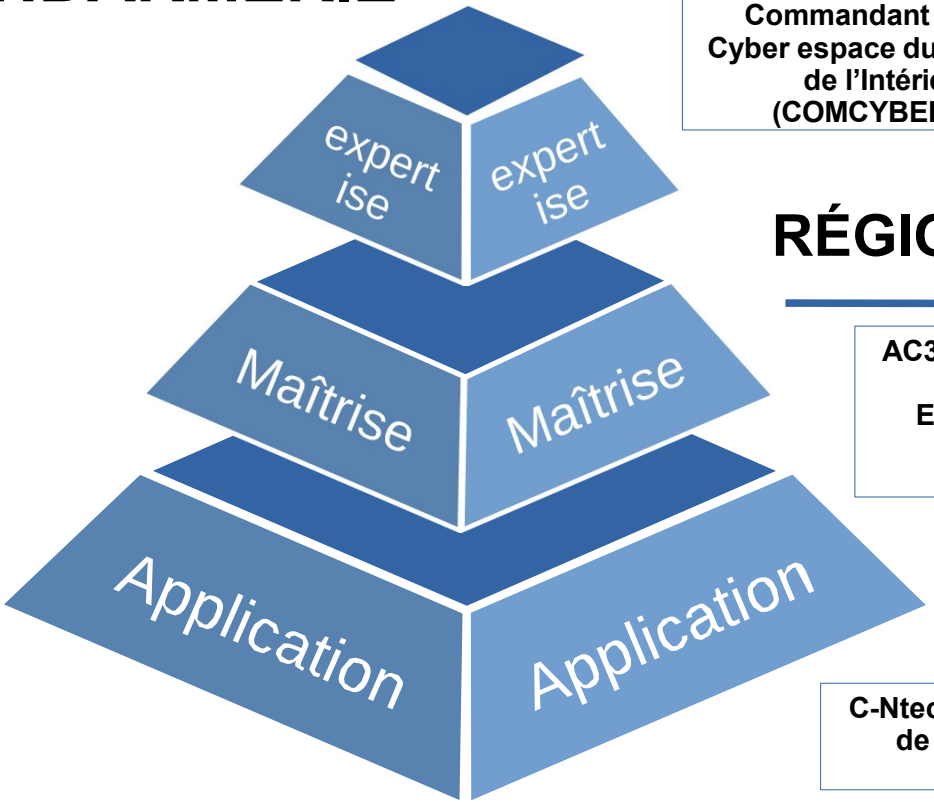
0805 29 29 40

PME / ETI

Collectivités / EPL

Associations

DISPOSITIF NATIONAL GENDARMERIE



NATIONAL

Commandant dans le Cyber espace du Ministère de l'Intérieur (COMCYBER_MI)

Unité Nationale Cyber (UNC)

Centre de lutte Contre la Criminalité Numérique (C3N)

RÉGIONAL / DÉPARTEMENTAL

AC3N – Conseiller cyber – Section Appui Judiciaire
Bureau Appui Numérique
Enquêteurs Nouvelles Technologies (NTECH) / Section Opérationnelle de Lutte contre les Cybermenaces (SOLC)

LOCAL

C-Ntech / Introduction aux Cyber Menaces – Brigades de recherches – Communeautés de Brigades – Brigades Territoriales

EN RGNA

- 1 OG conseiller cyber zonal
- 1 section cyber de 30 réservistes citoyens
- 1 AC3N, 4 SR
- 1 OG conseiller cyber et 1 SOG expert cyber dans chaque département
- 34 NTECH et 873 C-NTECH

RÉPARTIS DANS LES 12 DÉPARTEMENTS

L'OFFRE DE SERVICE GENDARMERIE

1 — AVANT LA CRISE

Sensibilisation, prévention, PCA/PRA

2 — PENDANT LA CRISE

Le dépôt de plainte, « 17 » en cas d'urgence

3 — APRÈS LA CRISE

Temps de l'enquête et de l'accompagnement

REMÉDIATION

JO 2024
ÉLECTIONS

Finalité lucrative

Campagne de déstabilisation

Opérations d'espionnage

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

POURQUOI DÉPOSER PLAINTE ?

VICTIME D'UNE CYBERATTAQUE

CONTACTER LE 17 OU LA BNUM SUR Ma Sécurité Site internet

Le dépôt de plainte permet L'INTERVENTION D'UN BINÔME ENQUÊTEUR / TECHNICIEN capable de conseiller sur les investigations numériques et les choix stratégiques à mener.
Des EXPERTS DE LA GESTION DE CRISE DE LA GENDARMERIE peuvent prendre en charge les interactions avec le cyberdélinquant.

Alerter au plus tôt c'est PRÉSERVER LES PREUVES NUMÉRIQUES pour identifier l'attaquant et bénéficier de conseils pour faire cesser l'attaque.
Anticiper le dépôt de plainte permet de faire gagner du temps.

La TRANSPARENCE implique la CONFIANCE.
L'intervention de la GN peut RASSURER l'éco-système de l'entreprise sur la gestion de l'incident.

L'intervention de la gendarmerie n'a AUCUN IMPACT sur la reprise d'activité. Les experts de la gendarmerie recueillent les éléments de preuves en étroite collaboration avec les équipes opérationnelles.

La victime conserve à tout instant la maîtrise de sa communication de crise.

Seul face à la crise ?
Une plainte, est-ce utile pour sortir de la crise ?
Perdre du temps précieux dans la crise
Risquer d'entâcher la confiance
Ralentir les actions de remédiation visant la reprise d'activité
Préserver l'image de l'entreprise

POUR AGIR ENSEMBLE
DÉPASSEZ VOS CRAINTES

Être reconnu en tant que victime
Agir en citoyen
Lutter contre la cyber-criminalité
S'entourer d'un allié dans la crise
Se protéger de futures attaques
Faire valoir ses droits

Victime mais pas coupable !
Le dépôt de plainte permet d'obtenir RÉPARATION DU PRÉJUDICE.

Le dépôt de plainte est le seul moyen D'INFORMER les forces de sécurité intérieur des menaces qui pèsent sur les citoyens.
Signaler c'est PROTÉGER ET PARTICIPER À L'EFFORT COLLECTIF.

Le dépôt de plainte permet de RECUEILLIR DES ÉLÉMENTS DE PREUVES NUMÉRIQUES qui permettent d'investiguer et peser sur les organisations cybercriminelles.

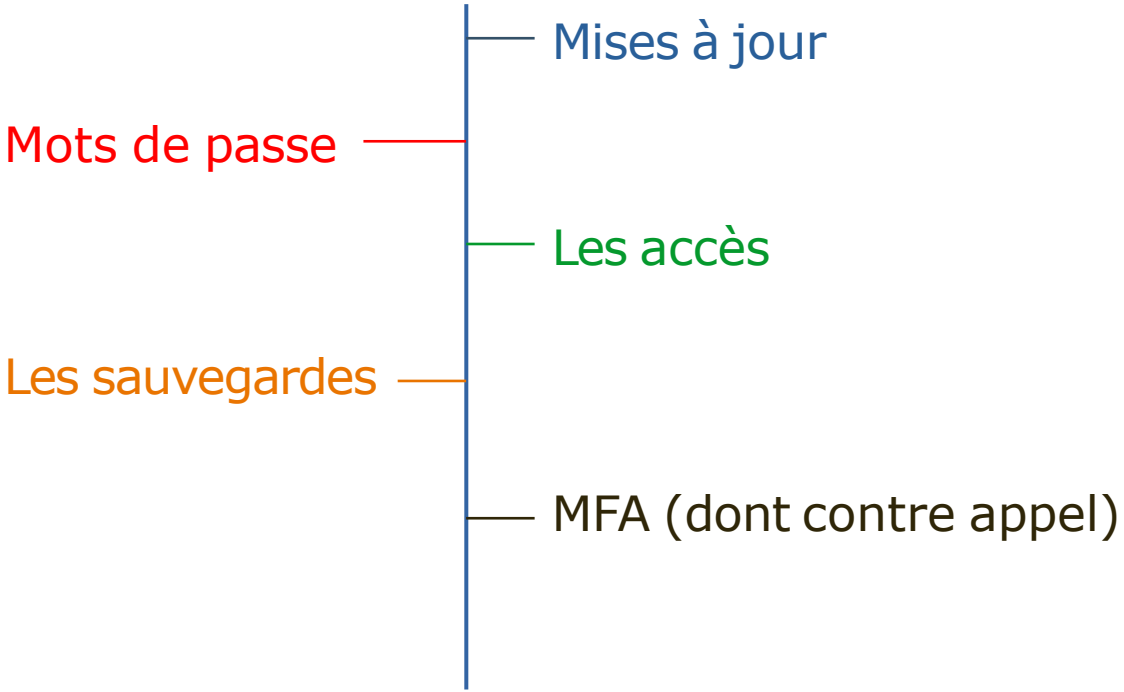
La gendarmerie vous ACCOMPAGNE DANS LA GESTION DE LA CRISE, grâce à des équipes projetables aux compétences intégrées, dédiées à l'identification des cybercriminelles.

Le dépôt de plainte permet de bénéficier de L'EXPERTISE DE LA GENDARMERIE dans la protection de l'entreprise.
La gendarmerie peut détenir des éléments permettant à l'entreprise de récupérer ses données en cas d'attaque par rançongiciel.

L'ASSURANCE CYBER permet à l'entreprise de limiter les conséquences économiques d'une cyberattaque.
La LOPMI (Art.5) soumet l'indemnisation des préjudices d'une cyberattaque au DÉPÔT DE PLAINTE DE L'ENTREPRISE.

Gendarmerie nationale

LES BONNES PRATIQUES



A RETENIR

2 Principes :

Prise de conscience => une attaque : PAS « SI » MAIS « QUAND »

L'attaquant est déjà dans votre SI

3 phases :

- Avant la crise
- Pendant la crise
- Après la crise

3 domaines d'action :

- Organisationnel
- Humain
- Technique

LIENS UTILES

- https://www.ssi.gouv.fr/
- https://www.cybermalveillance.gouv.fr/
- https://www.masecurite.interieur.gouv.fr/fr
- https://www.signal-spam.fr
- https://phishing-initiative.fr/contrib/
- https://signal.conso.gouv.fr/
- cyber-vigilance-nouvelleaquitaine@gendarmerie.interieur.gouv.fr

Questions - Réponses
Discussions

Association Française pour la Prévention des Catastrophes Naturelles et Technologiques
AFPCNT
Mieux comprendre, mieux prévenir
Soutenu par
MINISTÈRE DE LA TRANSITION ÉCOLOGIQUE ET DE LA COHÉSION DES TERRITOIRES
Liberté
Égalité
Fraternité

Merci à

Martin Veron
Ludovic Boncompain
Olivier Grall

Ghislaine Verrhiest-Leblanc
avec l'appui de Laurence Bonhomme et Virginie Perromat

Association Française pour la Prévention des Catastrophes Naturelles et Technologiques
AFPCNT
Mieux comprendre, mieux prévenir
Soutenu par
MINISTÈRE DE LA TRANSITION ÉCOLOGIQUE ET DE LA COHÉSION DES TERRITOIRES
Liberté
Égalité
Fraternité