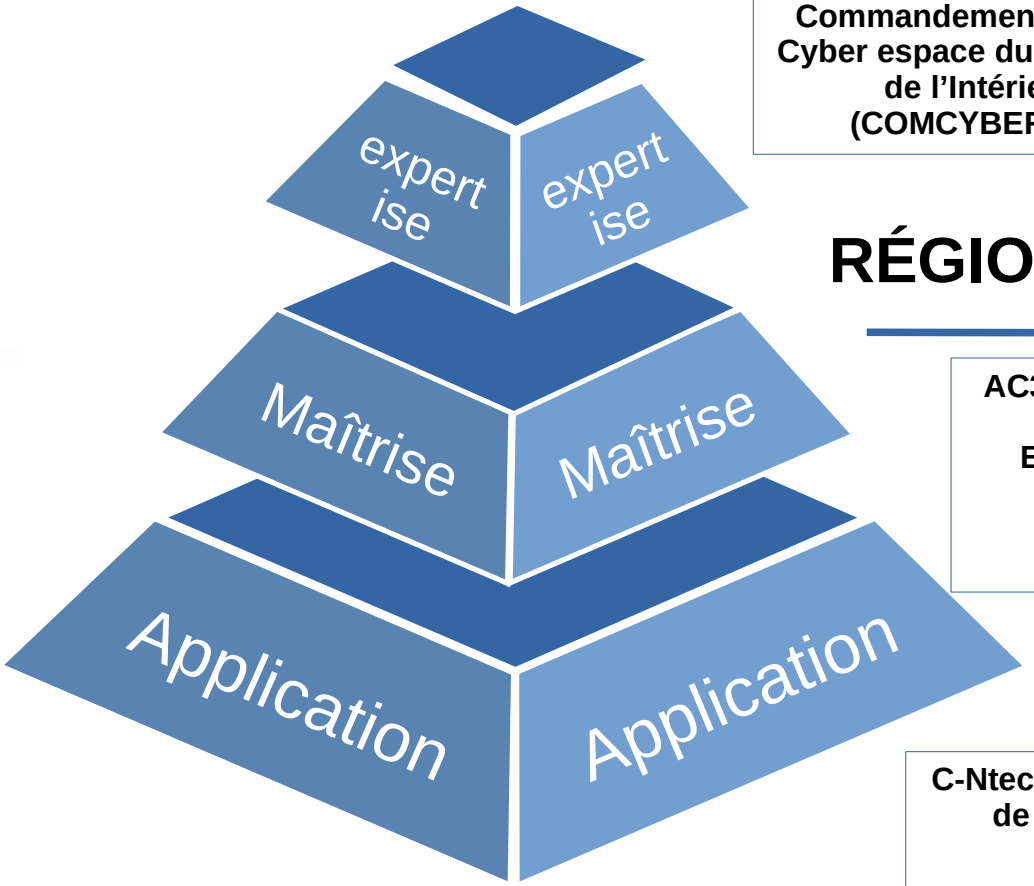
UNE CYBER ATTAQUE, ÇA N'ARRIVE PAS QU'AUX AUTRES...

DISPOSITIF NATIONAL GENDARMERIE



NATIONAL

Commandement 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 – Communautés de Brigades – Brigades Territoriales

EN RGNA

- 1 officier conseiller cyber zonal
- 1 section cyber de 30 réservistes citoyens
- 1 AC3N, 4 Sections de Recherches
- 1 officier conseiller cyber et 1 sous-officier expert cyber dans chaque département
- 34 NTECH et 873 C-NTECH

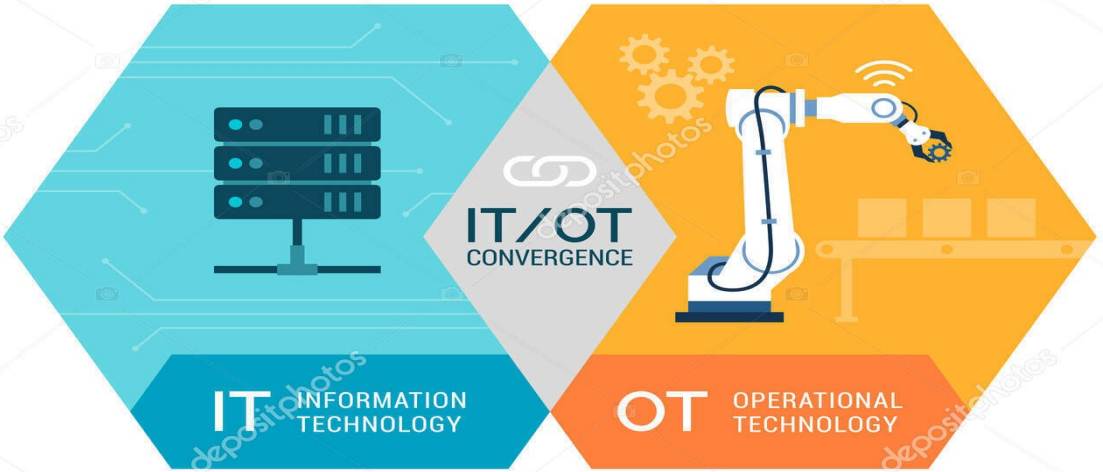
RÉPARTIS DANS LES 12 DÉPARTEMENTS

COMPRENDRE

cybersécurité des systèmes industriels (« Operational Technology ») - OT

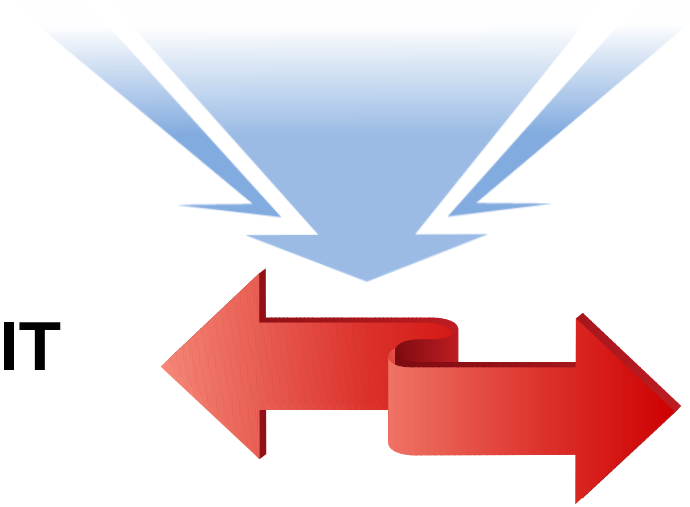
La convergence des univers IT (Information Technology) et OT

- **levier d’efficacité pour les processus et les métiers.**
- **mais également un facteur de cyber-risques.**



COMPRENDRE

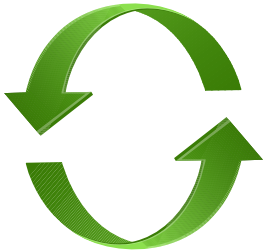
- **Le nombre de serveurs web,**
- **de sites distants,**
- **de télétravailleurs,**
- **d’objets connectés,**



RZO IT

RZO OT

FACTEURS DE VULNÉRABILITÉ



5 ans / 40 ans

- **L'AGE** : parc informatique IT / OT
- **Hardware / software** : maintien en condition de sécurité (MCS) / maintien en condition opérationnelle (MCO)
- **L'environnement** : contrôle d'accès moins aisé, conditions (poussière, humidité, températures …)
- **Priorités cyber** : OT → disponibilité, intégrité, confidentialité
  IT → confidentialité, intégrité, disponibilité

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 cyberdéliquant.

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 reccueillent les éléments de preuves en étroite collaboration avec les équipes opérationnelles.

La victime concerve 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

- Mises à jour
- Mots de passe
- Les accès
- Les sauvegardes
- MFA (dont contre appel)

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

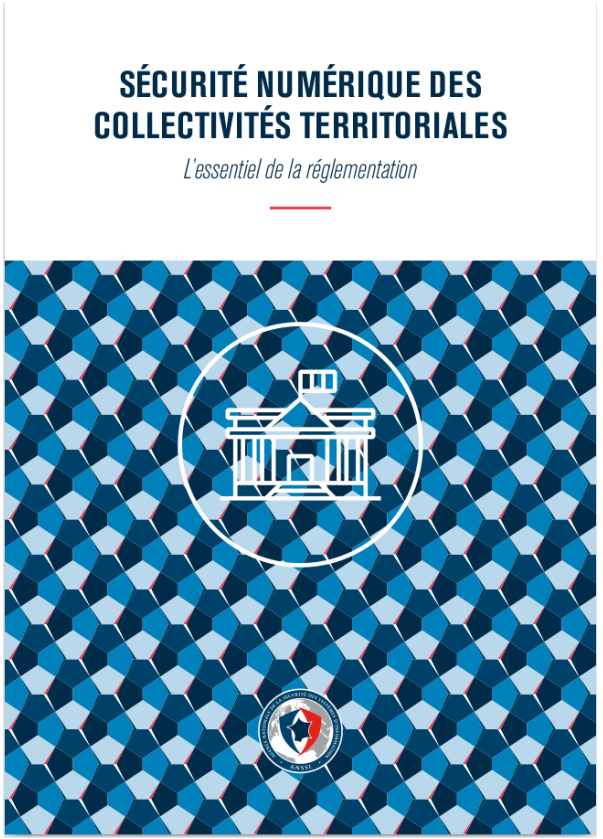
- https://www.ssi.gouv.fr/
- https://www.cybermalveillance.gouv.fr/
- https://www.masecurite.interieur.gouv.fr/fr
- https://www.signal-spam.fr
- https://phishing-initiative.fr/contrib/
- https://signal.conso.gouv.fr/
- cyber-vigilance-nouvelleaquitaine@gendarmerie.interieur.gouv.fr

LIENS UTILES

https://clusif.fr/publications/guide-cybersecurite-des-systemes-industriels-2021/

- cartographie des systèmes industriels ;
- appréciation des risques cyber ;
- architecture sécurisée ;
- intégration et recette de sécurité ;
- maintien en conditions de sécurité.

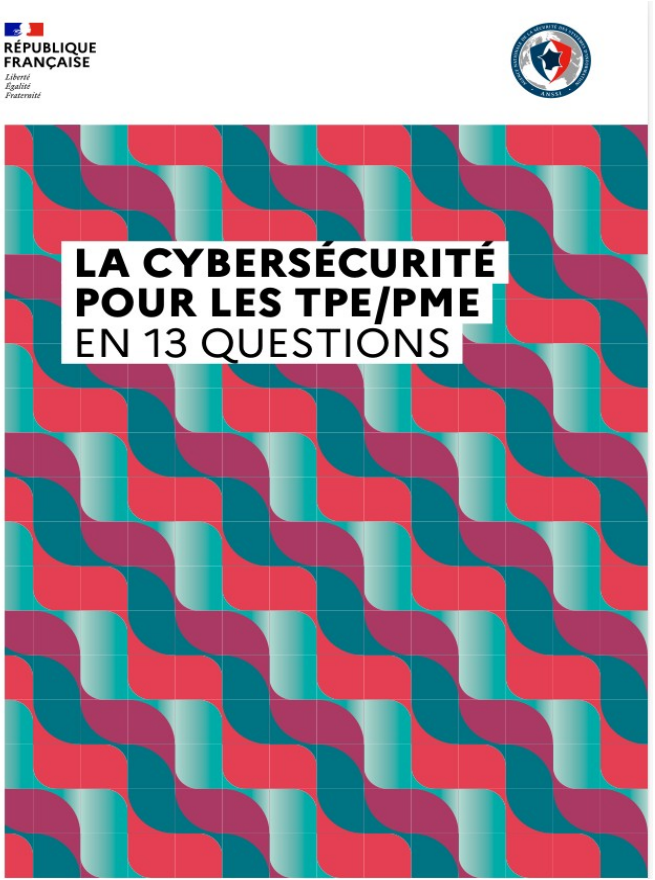
LIENS UTILES



https://www.ssi.gouv.fr/administration/guide/securite-numerique-des-collectivites-territoriales-lessentiel-de-la-reglementation/

https://www.amf.asso.fr/documents-cybersecurite-toutes-les-communes-intercommunalites-sont-concernees/40406

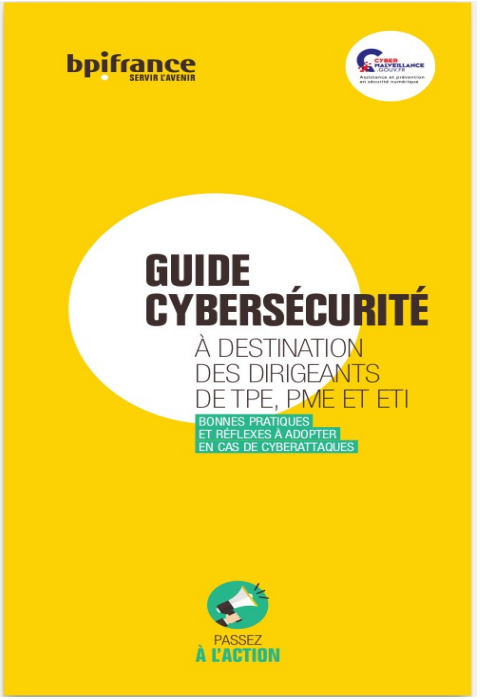
LIENS UTILES



https://www.ssi.gouv.fr/guide/la-cybersecurite-pour-les-tpepme-en-treize-questions/

LIENS UTILES

https://www.economie.gouv.fr/files/files/PDF/2017/bro-memento-cybersecurite-createur_0.pdf



https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/cybermalveillancegouvfr-bpifrance-guide-pme-tpe

QUESTION ?