FORUM DU RHIN SUPERIEUR SUR LES CYBERMENACES

18e édition

INSP Strasbourg

18 novembre 2025

EDITION 2025

ANIMATION

Madame Emmanuelle HAASER

Responsable veille et marketing
CCI Alsace Eurométropole
RC Gendarmerie nationale

Madame Noélie PLASSE

Responsable du pôle communication
Institut National du Service Public - INSP

Général Gwendal DURAND

Commandant le Groupement de Gendarmerie Départementale du Bas-Rhin

Monsieur Frédéric SPINDLER

Membre élu de la CCI Alsace Eurométropole, Vice-Président délégué à l'économie numérique
Dirigeant de Promoveo

Madame Irène WEISS

Conseillère régionale déléguée à la cybersécurité
Vice-présidente de la commission Enseignement supérieur, Recherche et Innovation

Monsieur Karl TERROLLION

Secrétaire général adjoint de la Préfecture du Bas-Rhin

BÂTIR UN ÉCOSYSTÈME NUMÉRIQUE SOLIDE ET SOUVERAIN POUR REPRENDRE LA MAIN SUR SON AVENIR DIGITAL

La souveraineté digitale s'impose aujourd'hui comme une priorité stratégique pour reprendre le contrôle de notre destin numérique.
Dans un monde où données, infrastructures et technologies sont devenues les moteurs du développement économique et de l'influence géopolitique, chaque dépendance technologique accroît notre vulnérabilité.
Cyberattaques, concentration du pouvoir numérique, fragilité des chaînes critiques : les menaces se multiplient et s'intensifient.
Experts, décideurs et acteurs de terrain sont réunit sur ce forum autour d'un enjeu central:
Comment garder la main sur nos choix technologiques et mieux gérer notre destin numérique ?
Les échanges porteront sur la protection des données sensibles, la sécurisation des systèmes, la réduction des dépendances et l'adoption de solutions fiables, éthiques et conformes aux standards européens.

La souveraineté numérique ne s'improvise pas : elle se construit pas à pas.
À travers des témoignages concrets, seront présentés des stratégies de résilience, des outils de cybersécurité et des modèles opérationnels alliant innovation, autonomie et durabilité.
La souveraineté numérique se construit par des choix éclairés, une gouvernance forte et une culture partagée de la sécurité.
Ce forum est l'occasion d'identifier des leviers d'action, de partager les meilleures pratiques et de coopérer autour d'une ambition commune : bâtir un numérique plus sûr, plus durable… et pleinement souverain.

Pascal MARY
Responsable cybersécurité - Hager Group
Enseignant en informatique - CCI Campus Alsace
RC Gendarmerie Nationale

PLAN DE SITUATION

INSP - 1 rue Sainte Marguerite à Strasbourg

Ad Honores
Réseau Alsace
5 rue du Nideck
67000 Strasbourg
www.adhonores.alsace

La gendarmerie et les officiers de la réserve citoyenne vous convient au

FORUM DU RHIN SUPERIEUR SUR LES CYBERMENACES

18ème édition

Mieux protéger votre destin numérique

TABLE RONDE 1 - ENJEUX ET MENACES
TABLE RONDE 2 - LEVIERS ET SOLUTIONS

Entrée libre
Demande d'inscription sur
www.adhonores.alsace

18 NOVEMBRE 2025

auditorium de l'INSP
1 rue Sainte Marguerite à Strasbourg

FRC 2025
18ème édition

PARTENAIRES

SPONSORS

Nos partenaires

FRC
Forum Cybermenace

INSP
Institut national
du service public

Nos partenaires

Nos partenaires

Nos partenaires

Nos partenaires

Nos partenaires

CRCC
COMPAGNIE REGIONALE DES COMMISSAIRES AUX COMPTES
COLMAR

Nos partenaires

Nos partenaires

Nos partenaires

ORDRE DES EXPERTS-COMPTABLES

Région Grand Est

La Gendarmerie, la RCDS et Ad honores - Réseau Alsace

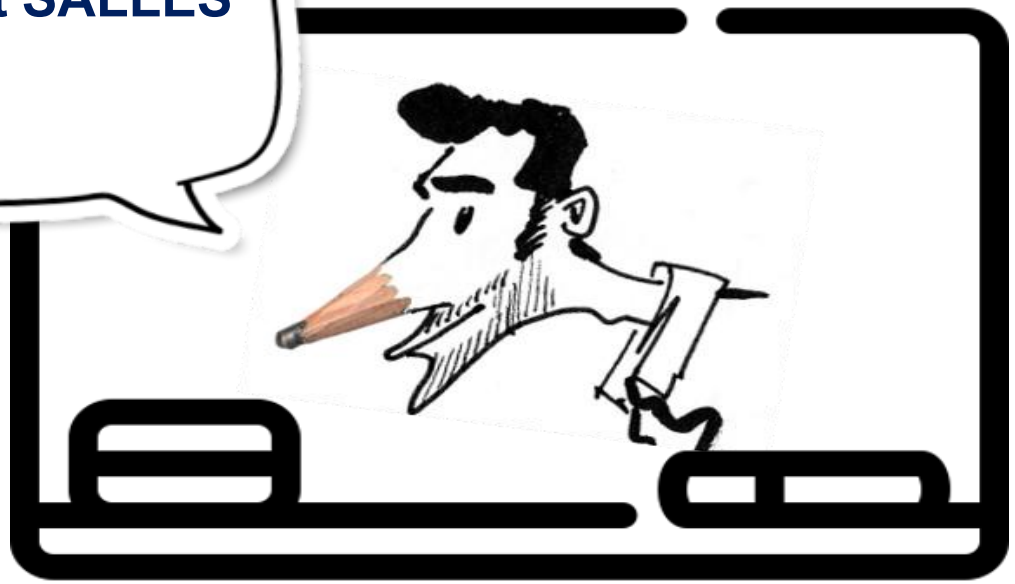
Notre objectif

Mobiliser les décideurs d'entreprises sur les enjeux de la cybersécurité afin de leur permettre d'en être plus acteur

Notre fidèle dessinateur

FRC
Forum Cybermenace

Laurent SALLES



Connexion wifi

Connexion au réseau Wifi : WIFI_INSP

Identifiant : **forumcybermenace**

Mot de passe : **pX6Xzg89**

Profil : **EVENEMENT**

Dans le respect de la charte informatique de l'INSP

Conférence plénière

Souveraineté numérique : mythe ou réalité

Quelles réponses européennes ?

Par Myriam QUÉMÉNER

EDITION 2025

Madame Myriam QUÉMÉNER

Avocat général honoraire – Docteur en droit

Définition

La souveraineté numérique désigne la capacité d'un État à contrôler ses infrastructures, ses données et ses technologies numériques.

Dans un monde dominé par les géants du numérique, cette souveraineté devient un enjeu stratégique.

Apparition du terme dans les années 2000, avec la montée en puissance des GAFAM.Révélations d'Edward Snowden (2013) ont renforcé les inquiétudes sur la surveillance numérique.

Depuis, les États cherchent à reprendre le contrôle sur leurs données et infrastructures.

Les enjeux

Sécurité nationale : protection contre les cyberattaques.

Protection des données personnelles : éviter la fuite vers des serveurs étrangers.

Indépendance technologique : limiter la dépendance aux logiciels et matériels étrangers.

Préservation des valeurs démocratiques : encadrer les algorithmes et les plateformes.

Les défis actuels

Dépendance aux GAFAM : hébergement, logiciels, réseaux sociaux.

Fragmentation du web : vers un internet à plusieurs vitesses.

Manque de transparence : algorithmes opaques, biais.

Retard technologique : difficulté à concurrencer les leaders mondiaux.

Les acteurs concernés

États : législateurs, régulateurs, agences de cybersécurité.

Entreprises : fournisseurs de cloud, développeurs de logiciels, startups.

Citoyens : utilisateurs, consommateurs, électeurs.

Organisations internationales : ONU, UE, OCDE.

Cadre juridique et règlementaire

RGPD (UE) : encadrement du traitement des données personnelles.

Cloud Act (USA) : accès des autorités américaines aux données stockées à l'étranger.

Initiatives françaises : cloud souverain, cybersécurité, plan France Num.

Réponses envisageables

01

Investir dans les infrastructures locales : data centers, réseaux.

02

Favoriser les logiciels libres et européens.

03

Former les citoyens au numérique responsable.

04

Renforcer la coopération internationale sur la cybersécurité et les normes.

Perspectives : la souveraineté numérique, une priorité gouvernementale

Vers un internet plus souverain, mais aussi plus fragmenté ?

L’intelligence artificielle : nouveau champ de bataille géopolitique.

L’équilibre entre ouverture, innovation et protection reste à inventer.

L’apport de la loi SREN

La loi SREN de mai 2024 y a inscrit l’exigence de souveraineté

Toute donnée relevant d'un secret protégé par la loi et dont la violation pourrait porter atteinte à l'ordre public doit être hébergée de manière souveraine, avec la **qualification SecNumCloud** de l'Anssi. La France n'a pas réussi à imposer ses critères de souveraineté dans la certification européenne des services de cloud (EUCS), toujours en discussion.

Exemple de souveraineté : France connect

FranceConnect incarne l'une des réussites de la politique de souveraineté numérique. Lancé par la Dinum pour contrer les systèmes d'authentification de Facebook et Google, ce connecteur est aujourd'hui massivement utilisé, même si les petites collectivités peinent à le déployer, du fait notamment des frais d'intégration demandés par les éditeurs.

La Cour regrette néanmoins que la Dinum soit "dépendante de ses prestataires". Cette dépendance fragilise la maîtrise d'un dispositif conçu pour garantir la souveraineté de l'identité numérique des citoyens. Elle expliquerait en partie la réaction tardive de l'État face aux usurpations d'identité massives de 2022 qui a débouchée sur la mise en place de France Connect+ et d'une cellule de sécurité dédiée. La Cour recommande à la Dinum de professionnaliser sa stratégie de lutte contre la fraude en s'inscrivant dans le programme de travail de la mission interministérielle de lutte contre la fraude (Micaf), qui coordonne les administrations en matière de fraude aux finances publiques.

Pour aller plus loin

CNIL, ANSSI, Commission européenne

Rapports : "Souveraineté numérique" (Institut Montaigne), "Cloud souverain" (Senat)

Baromètre de la souveraineté numérique 2025

https://www.ey.com/content/dam/ey-unified-site/ey-com/fr-fr/services/cybersecurity/documents/ey-barometre-de-la-souverainete-numrique-sep-2025.pdf

Rapport de la cour des comptes sur la souveraineté numérique 2025

Merci de votre attention

On sait mais on ne fait pas !

Philippe Van GOOSSENS WOUTERS

Expert en comportement de sécurité - CBC

Table ronde 1

Enjeux et menaces

Elena VALLEJO
Sébastien DUPENT
Anthony CHARREAU
Damien ERNST
Patrick ARNOULD
Ludovic HAYE

EDITION 2025

Crise en réseau : maîtriser ou subir

Madame Elena VALLEJO

Consultante Cybersécurité - Acesigroup

Monsieur Sébastien DUPENT

Professeur agrégé en Economie et Gestion spécialité système d'information - Spécialiste cybersécurité - Lycée René Cassin
RC Gendarmerie nationale

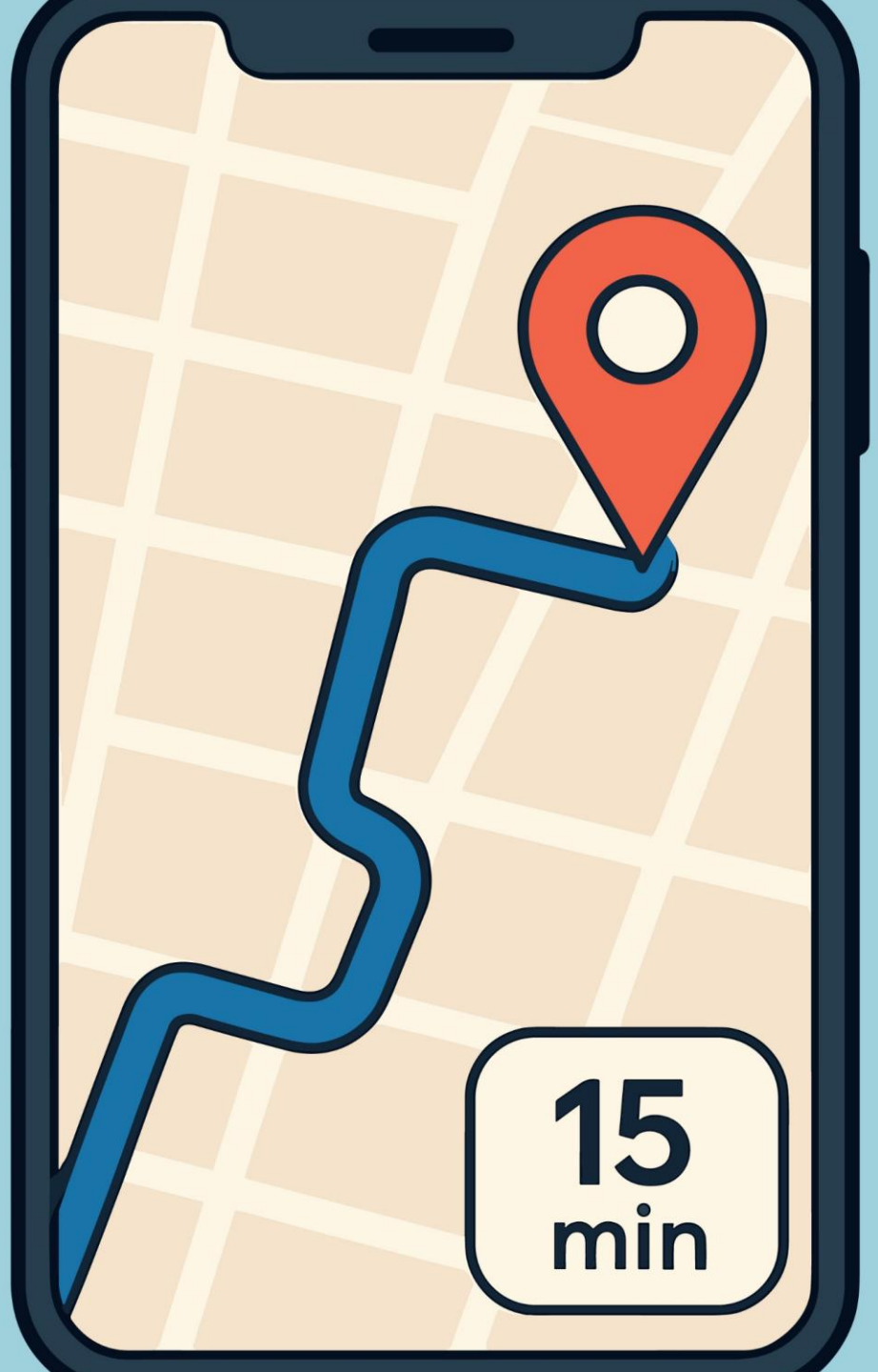
Organiser sa résilience numérique et anticiper la crise : est-ce vraiment indispensable ?

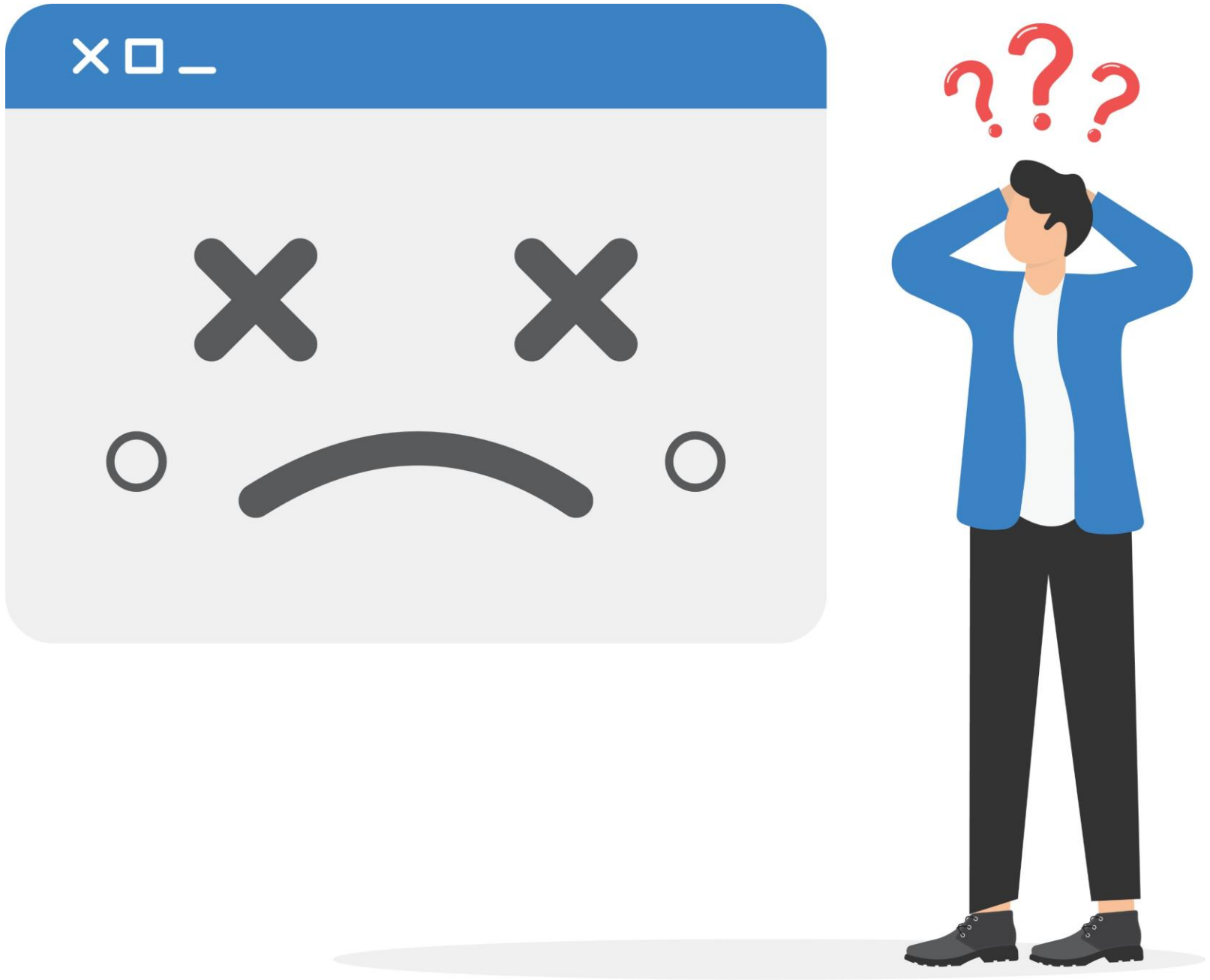
Monsieur Anthony CHARREAU

Responsable cybersécurité

Notre monde actuel est profondément digital


10
14
17


15
min



Notre monde va vite

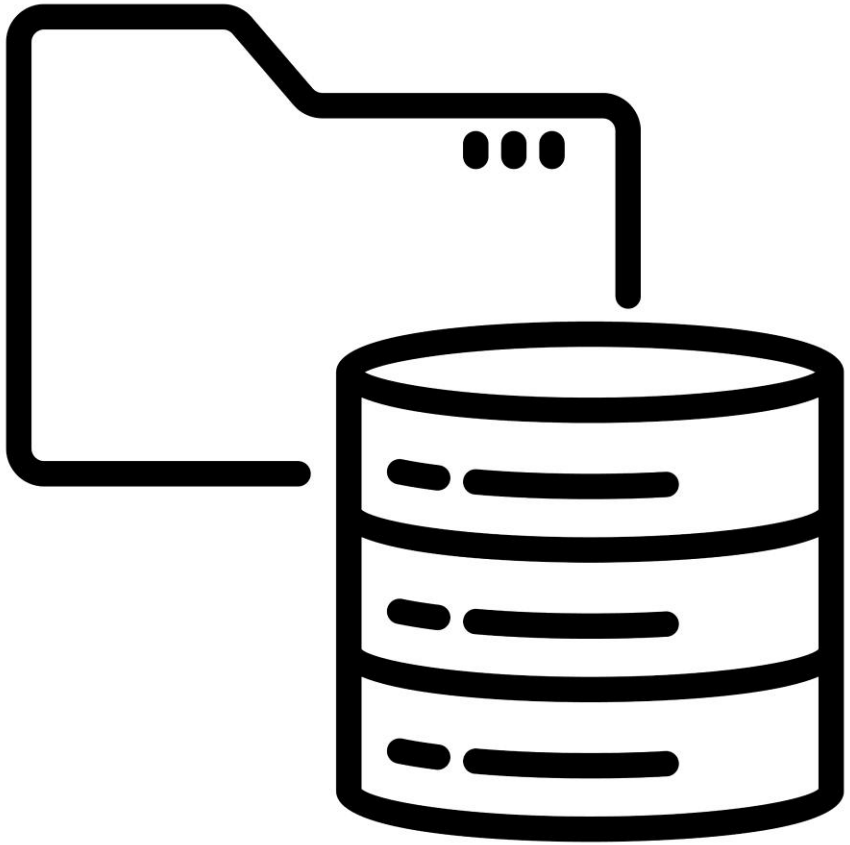

RANSOMWARE
RANSOMWARE
RANSOMWARE
RANSOMWARE
RANSOMWARE

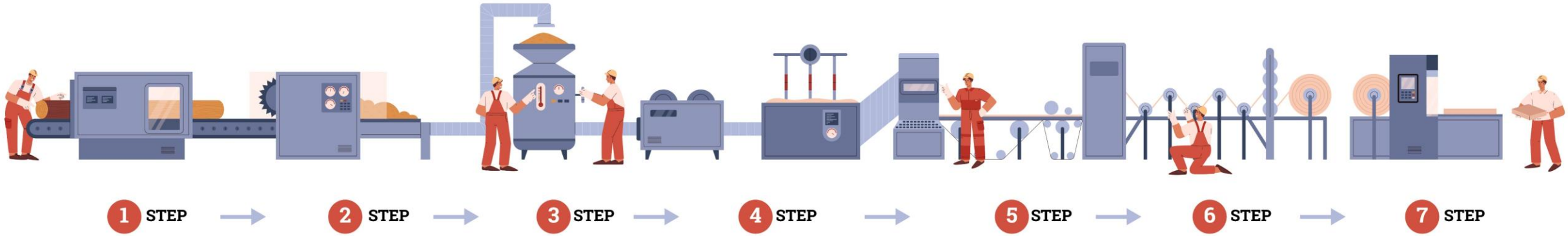
Il ne faut pas avoir peur du digital et d'internet

Le système d’information

Et si l'informatique ne fonctionne pas ?

Le nerf de la guerre #1 : les données




1 STEP
2 STEP
3 STEP
4 STEP
5 STEP
6 STEP
7 STEP


BACKUP

Le nerf de la guerre #2 : l'anticipation


SOLUTION
PROBLEM

Le nerf de la guerre #3 : la théorie mais aussi … la pratique par l'entrainement

Puis une logique d'amélioration continue

« L'informatique n'est pas qu'un centre de cout, c'est surtout un formidable vecteur de différentiation »

Maîtriser ses coûts dans la durée

Monsieur Damien ERNST

Cadre dirigeant informatique (secteur privé)
Auditeur 2ème session nationale de l'IHEDN au sein de la 5ème majeure « souveraineté numérique et cybersécurité »
RC Gendarmerie nationale

Souveraineté numérique et maîtrise des coûts

5 435 Mds $
Dépense IT mondiale en 2025

265 Mds €
Dépense de l'UE pour des services Cloud américains

- Dépendance croissante des entreprises aux services numériques:
  - L'outil de production repose de plus en plus sur le numérique
  - Le cœur de business est tributaire du système d'information et des services numériques
- Enjeux de « souveraineté » pour l'entreprise :
  - Garantir le fonctionnement de l'outil de production
  - Assurer disponibilité et qualité des services aux clients
  - Préserver la compétitivité de l'entreprise
- Maitrise impérative des services numériques, y compris d'un point vue économique

Services numériques externalisés

La promesse du cloud

- Facturation à la consommation
- Ressources IT « illimitées »
- Catalogue de services
- Services « managés »

Les risques financiers

- Prédictibilité réduite des coûts
- Perte des droits d’utilisation
- Surcoût des abonnements sous-utilisés

Evaluation des coûts : intrants à considérer

- L'intérêt et le coût d'une solution numérique s'évaluent sur la base du TCO (Total Cost of Ownership)

$$TCO = CAPEX + OPEX$$

- Ne pas négliger les coûts d'intégration ni la perte éventuelle de productivité des utilisateurs par manque d'intégration du service dans le S.I. de l'entreprise
- Considérer la durée pendant laquelle sont garanties les conditions financières négociées
- Inclure les conditions et frais de sortie

Quelques leviers de souveraineté

Dans tous les cas de figure :

→ Adapter les choix en fonction des enjeux/risques business

→ Mettre les fournisseurs en concurrence

→ Adopter du « dual sourcing » (services les plus critiques)

Services numériques externalisés :

→ Vérifier la réversibilité (récupération des données)

→ Vérifier la portée des certifications affichées
(une non-conformité peut engendrer des risques financiers)

→ Vérifier l'applicabilité des « EU Clauses »

Services numériques internes :

→ Sécuriser les contrats: durée longue, conditions de prolongation et de sortie

→ Intégrer des clauses de maintien de la solution « on premise »

→ Clause de séquestre (situations particulières)

→Logiciels libres : coûts indirects
+ risques cyber et opérationnels

CONCLUSION

MAÎTRISER LES CHOIX ET LES COÛTS DES SERVICES NUMÉRIQUES DE L'ENTREPRISE …

… CONTRIBUE À LA MAÎTRISE GLOBALE DU BUSINESS ET À LA PÉRRENITÉ DE L'ENTREPRISE

Du panorama juridique à la réalité et aux pratiques

Monsieur Patrick ARNOULD

Consultant Protection des données & Sécurité des informations – Acesigroup

DPO externe, CIPM, CIPP/E, ISO27001 LI/LA, ISO27005 RM, NIS2 LI

Sommaire de l’intervention

- ➢ Préambule
- ❑ (Tentative de) Panorama juridique, général et sectoriel
- ❑ Compréhension et effectivité de la mise en œuvre sur le terrain
- ❑ Et demain… ?

1. Préambule important

Consultant = pas avocat, ni juriste, ni autre forme de conseil juridique !

- Ceci n'est pas un conseil juridique, juste une vision personnelle basée sur le retour d'expérience d'un consultant
- Le panorama n'a pas vocation à être exhaustif

→ Adressez-vous à votre conseil juridique !

Sommaire de l'intervention

- ✓Préambule
- ➢(Tentative de) Panorama juridique, général et sectoriel
- ❑Compréhension et effectivité de la mise en œuvre sur le terrain
- ❑Et demain… ?

2. Tentative de panorama législatif & règlementaire

Parmi les textes fondateurs et toujours en vigueur :

- ✓Loi 78-17, Informatique & Libertés (LIL)
- ✓Loi 88-19, Loi Godrain, fraude informatique (CP 323-1 s.)
- ✓Loi 2004-575, confiance en l'économie numérique (LCEN)
- ✓Décret 2006-580, Convention de Budapest sur la cybercriminalité
- ✓Code de la Propriété intellectuelle (CPI)
- ✓Code de la Santé Publique (CSP)
- ✓Code de la Défense et Lois de programmation militaire 2013 et 2019
- ✓Code des Postes et Communications Electronique (CPCE)
- ✓Loi 2023-1322, facturation électronique…
- ✓Rappel sur les obligations de signalement aux autorités

Repositionner l'UE dans la course mondiale sur le numérique et la donnée

Rappel quant aux obligations de signalement

Obligation de signaler les incidents survenus :

- Aujourd'hui à l'ANSSI si vous êtes désignés OIV ou OSE ou FSN
- aux autorités de protection des données, si données personnelles en jeu
- aux personnes concernées, qu'elles puissent prendre des mesures
- aux ARS, dans certaines situations (atteinte à des systèmes / données de santé)
- aux (cyber)assureurs, pour pouvoir être couverts / dédommagés
- Demain, au CSIRT si vous êtes/serez une EE/EI dans le périmètre NIS2/Loi Résilience

ATTN aux injonctions parfois contradictoires concernant l'ordre dans lequel faire ces notifications et les délais de notification initiale après prise de connaissance

Sans oublier la question du dépôt de plainte auprès des services spécialisés lorsque l'incident fait suite à un acte malveillant

2. Tentative de panorama législatif & règlementaire

Parmi les dernières évolutions des dernières années :

- ✓ Data Governance Act (**DGA**) : accessibilité et usage des données du secteur public
- ❑ Data Market Act (**DMA**) : pour les « grandes plateformes technologiques »
- ✓ Data Act (**DA**) : accès et usage des données du secteur privé
- ✓ Data Services Act (**DSA**) : transparence, publicité en ligne, contenus illégaux…
- ✓ Artificial Intelligence Act (AIA ou **RIA**) : développement, usage de l'IA…
- ✓ CyberResilience Act (**CRA**) : sécurisation des produits et services connectés
- ✓ Network and Information Security (**NIS2** ou SRI2) : sécurisation des activités essentielles à la société
- ✓ Digital Operational Resilience for the financial sector Act (**DORA**) : secteur financier
- ✓ Résilience des entités critiques (**REC**) : résilience « physique » d'infrastructures essentielles
- ❑ European Health Data Space (EHDS) : accessibilité et usage des données de santé
- ❑ Responsabilité du fait des produits défectueux…

Repositionner l'UE dans la course mondiale sur le numérique et la donnée

Tentative de panorama législatif & règlementaire

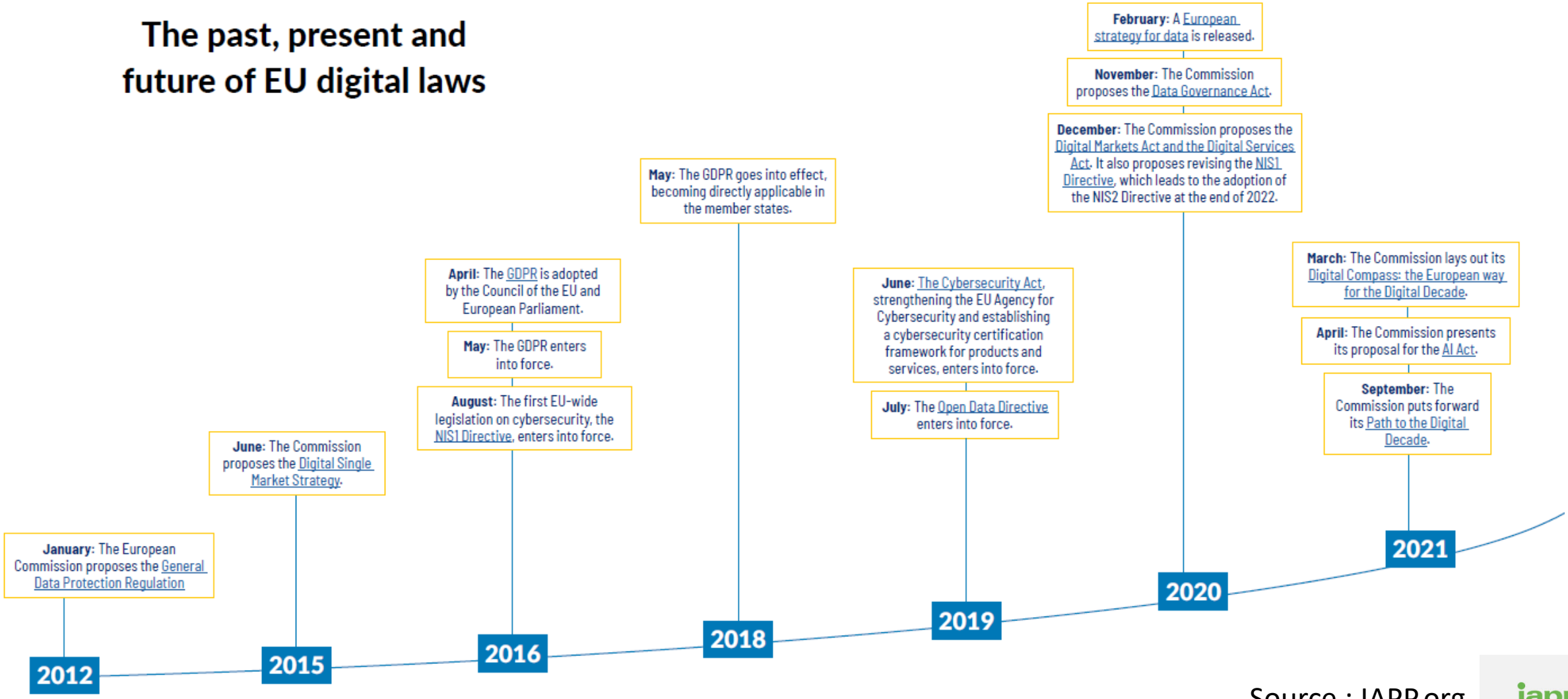
En guise de conclusion sur cette partie

- « mille-feuilles règlementaire et normatif »
- Accélération, multiplication et complexification des textes (p. suivantes)
  - Stratégie de (re)positionner l'Union Européenne dans la course mondiale sur le numérique et les données
  - Nécessité d'accélérer et harmoniser la « transition numérique » au sein de l'ensemble des états membres de l'UE
  - Volonté de réguler pour encadrer les « mauvaises pratiques » qui perdurent car l'écosystème ne s'autorégule pas seul

→ élever le niveau de confiance dans le numérique et libérer le potentiel d'innovation via la réutilisation des données !

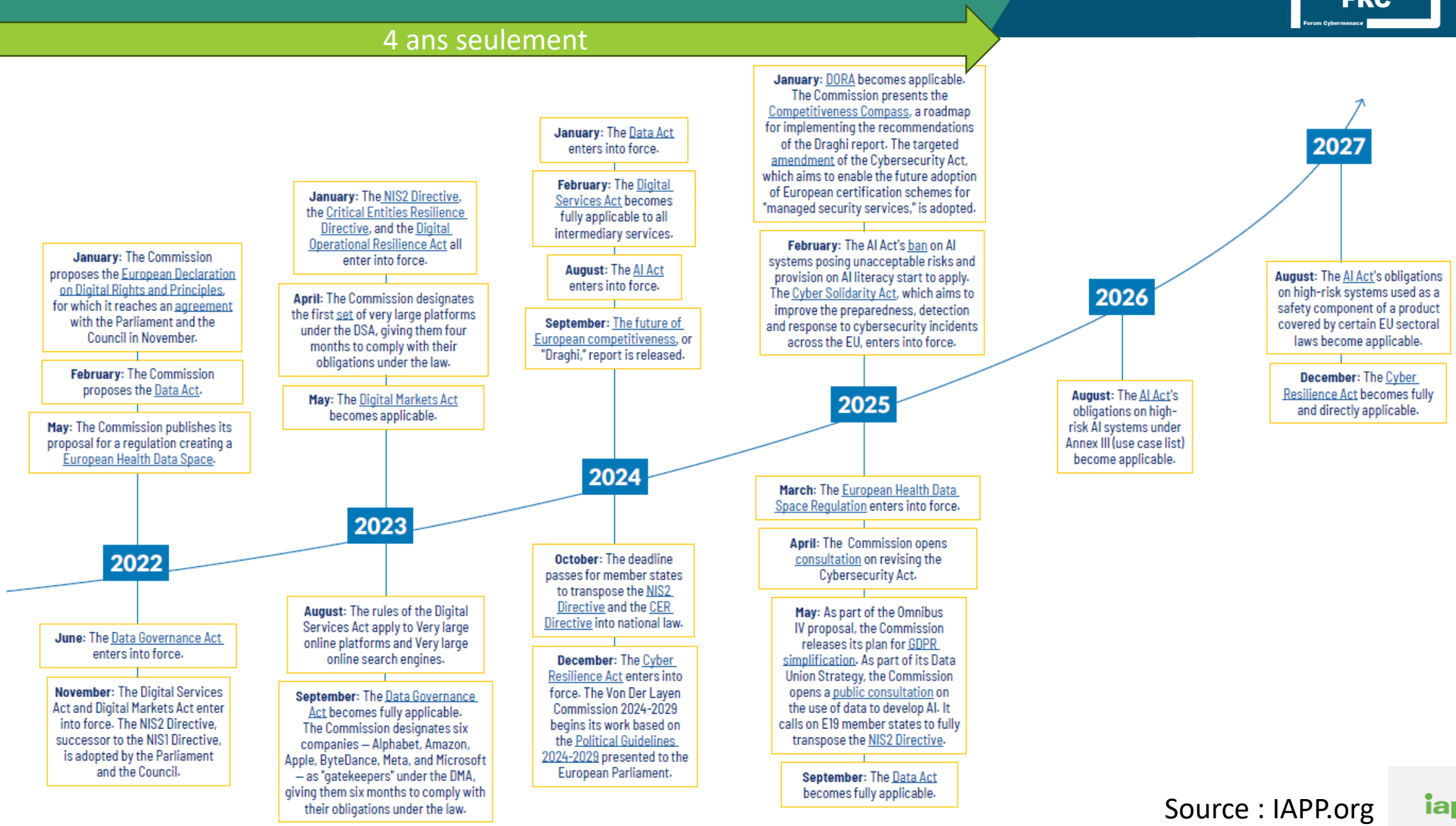
10 ans

The past, present and future of EU digital laws



Source : IAPP.org

4 ans seulement



Source : IAPP.org

Sommaire de l'intervention

- ✓Préambule
- ✓(Tentative de) Panorama juridique, général et sectoriel
- ➢Compréhension et effectivité de la mise en œuvre sur le terrain
- ❑Et demain… ?

3. Quel écho sur le terrain ?

On est bien loin de tout ça…

Les chefs d'entreprise / Comité de Direction des PME/PMI/ETI, ainsi que les acteurs publics sont peu familiers de ces textes, de leurs motivations, ambitions, et obligations associées

- DSI/RSI/RSSI et/ou conseils externes qui les informent
- Peu d'anticipation
- Obligations perçues comme des **freins** éloignées du terrain et des affaires,
- Sans en percevoir, ou rarement, le bénéfice pour l'entreprise, sa vie, voire sa survie et sa résilience
- Certaine frilosité voire une **réticence certaine** à procéder aux **obligations de notifications aux autorités**,
- Même approche pour faire un **dépôt de plainte** lorsque cela est pertinent
- …

3. Quel écho sur le terrain ?

Alors, quelle approche avoir ?

- Identifier les textes applicables, leur périmètre, leurs objectifs…
- Dresser un état des lieux (« *gap analysis* »)
- Les considérer comme des **vecteurs de compétitivité**
  - Respect sera de plus en plus évalué voire audité… et les manquements sanctionnés
- Engager une réelle démarche projet de mise & maintien en conformité…

- Certains textes (ex NIS2) prévoient une obligation « d'**acculturation** » des dirigeants, afin qu'ils appréhendent mieux le sujet des risques numériques aux fins de mieux les gérer

Sommaire de l'intervention

- ✓Préambule
- ✓(Tentative de) Panorama juridique, général et sectoriel
- ✓Compréhension et effectivité de la mise en œuvre sur le terrain
- ➢Et demain… ?

4. Et demain… ?

A noter dans le « Programme de travail 2025 de la Commission » (lien)

- La volonté clairement marquée de **maintenir un effort sur le numérique** :
  - « *préserver les actifs, les intérêts, l'autonomie et la sécurité stratégiques, et éviterons toute situation de dépendance stratégique à l'égard de sources hors UE…*»
  - « *mieux protéger et renforcer la résilience des infrastructures physiques et numériques…* »

Et de nouvelles initiatives déjà connues

- Le "**Digital Simplification Omnibus** », prévu d'être dévoilé le 19.11,
- Le "Digital Networks Act" qui concernera le secteur des télécoms, prévu d'être publié en Décembre, et qui serait une "refonte" du Code des communications électroniques de l'UE
- Etc.

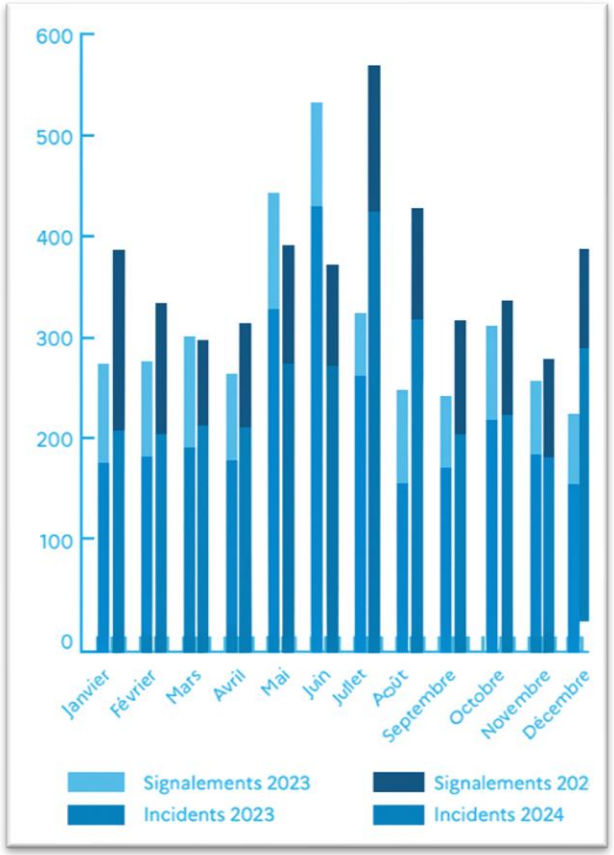
La confiance en première ligne

l'enjeu caché de la gestion des cybercrises

Monsieur Ludovic HAYE

Sénateur du Haut-Rhin, membre de la commission des affaires étrangères, de la défense et des forces armées
Conseiller Régional
RC Gendarmerie National

Hausse significative des cyberattaques



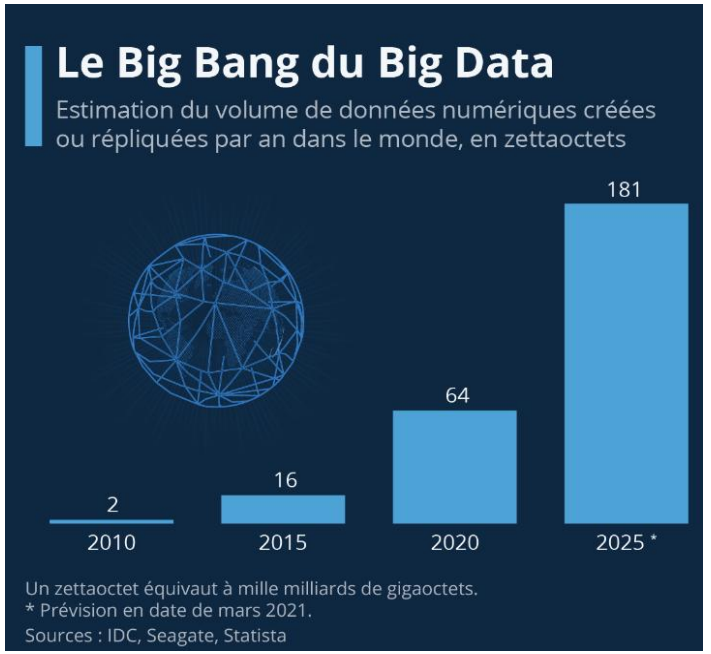
En 2024, **67% des entreprises** ont enregistré une **hausse des cyberattaques.**

Pourtant…

→ **1/3 des dirigeants** reconnaissent ne pas être prêts face aux cyberattaques.

→ **44% des entreprises** utilisant l'IA ignorent leur exposition réelle aux risques.

Mais la multiplication des risques force une prise de conscience.

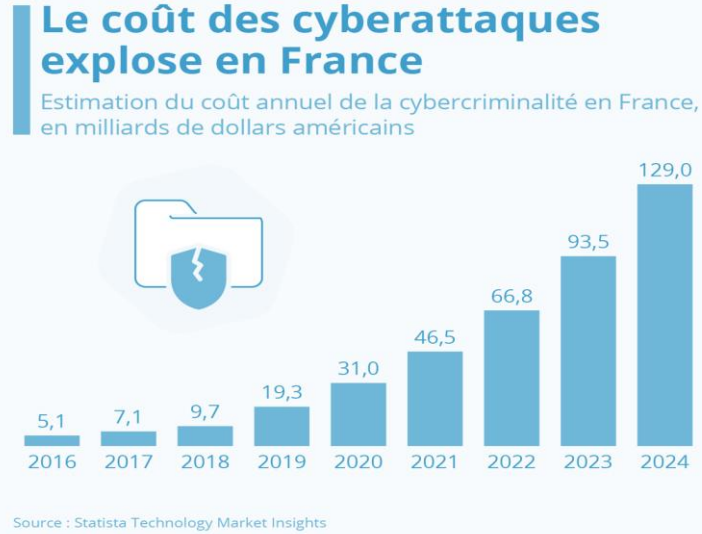


Pourquoi se protéger ? Les attaques cyber – un risque réel pour les Entreprises

Exemple de l'attaque de Colonial Pipeline aux États-Unis en 2021 : une attaque par ransomware qui paralyse les systèmes informatiques, forçant l'arrêt du transport de carburant dans le sud-est du pays.

- L'état d'urgence est déclaré par Joe Biden
- La crainte d'une pénurie entraine une hausse des prix = fermeture de 15 000 stations-service
- L'entreprise paye une **rançon de 4,4 millions de dollars** pour rétablir son système informatique.

→ Le coût moyen d'une cyberattaque est de **15 000€** pour une entreprise. Une entreprise sur 8 rapporte des coûts dépassant les **200 000€.**



Cybersécurité et IA : un duo stratégique.. et risqué

→ **44% des entreprises** utilisant l'IA ignorent leur exposition réelle aux risques.
→ l'IA est intégrée dans des fonctions critiques (détection d'intrusions, automatisation des réponses, analyse prédictive RH, finance, logistique).

Deepfake : la cyberattaque à 25 millions de dollars (Hong Kong)
En 2024, une entreprise multinationale a perdu 25 M$ lors d'une visioconférence où les participants étaient… des avatars IA. Des cybercriminels ont recréé les visages et les voix de plusieurs dirigeants pour convaincre un employé de transférer les fonds
→ Voix clonées, visages recréés, instructions crédibles.
→ Le transfert a été validé sans soupçon.

“Rebâtir la confiance après une cyberattaque” : les étapes « clés»

→ 1. **Le CHOC,** le constat, l’état des lieux

Message clé :

- Une cyberattaque ne touche pas seulement les machines.

- Elle atteint ce que nous avons de plus précieux : la confiance.

→ 2. La **transparence**, notre première réponse

Message clé : **La confiance ne se décrète pas, elle se reconstruit - les lignes de code après la ligne de conduite.**

- Ni silence, ni dissimulation

→ 3. Les **actions immédiates**

Message clé : **Nous avons transformé un incident en accélérateur de maturité numérique.**

- Activation du plan de continuité
- Coopération avec l’ANSSI, les autorités
- Audit complet des infrastructures
- Renforcement de nos protections et de notre gouvernance.

“Rebâtir la confiance après une cyberattaque” : les étapes « clés»

→ 4. L’**HUMAIN** au cœur de la résilience

Message clé : **La cybersécurité n’est pas qu’une affaire d’outils, c’est une culture partagée, une vigilance collective.**

- Trahis par la technologie**, les femmes et les hommes de l’entreprise** ont tenu bon.

→ 5. **Retisser** le lien de confiance

Message clé : **« Ce n’est pas la cyberattaque qui nous définit, mais la manière dont nous y avons répondu. »**

- Nos clients, nos partenaires, nos salariés nous ont soutenus, parfois dans le doute, mais toujours dans l’exigence. (loyauté Vs infaillibilité).

→ 6. Un **engagement** durable

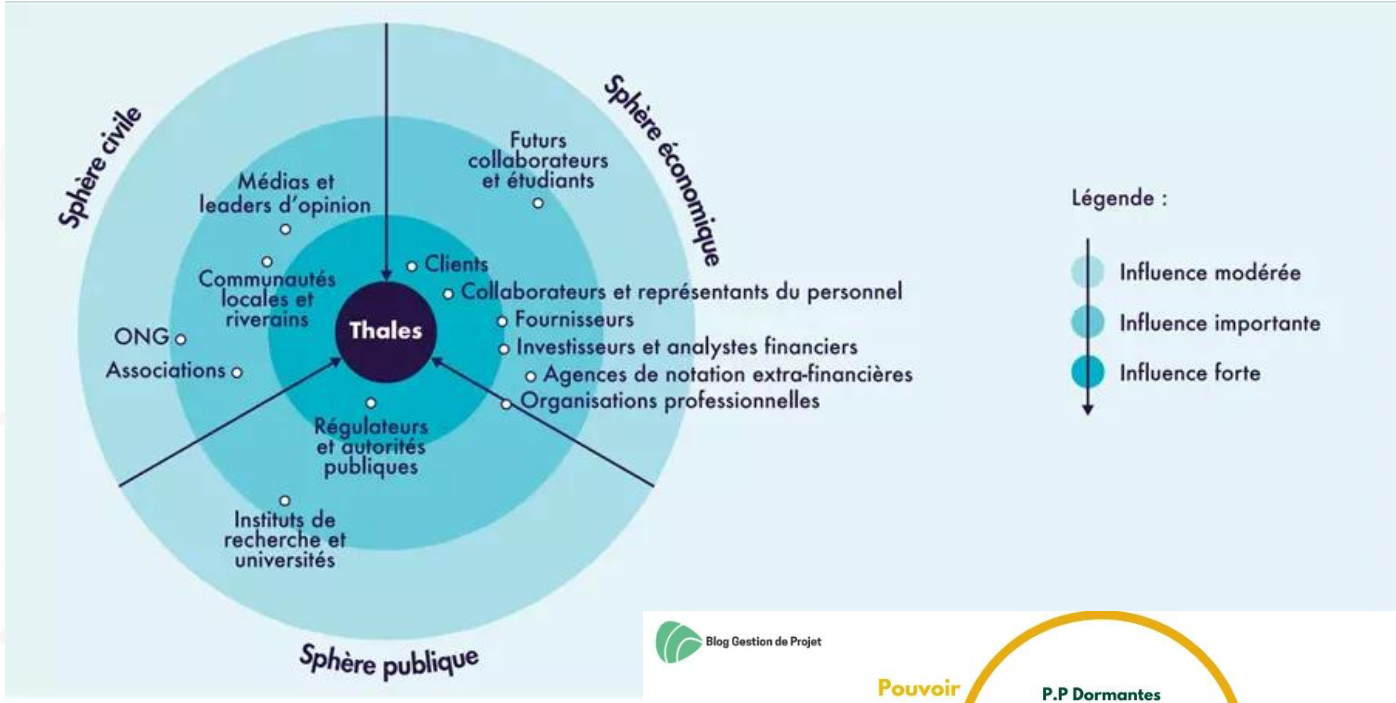
Message clé : « **Nous avons fait de la cybersécurité une valeur, pas une variable.** »

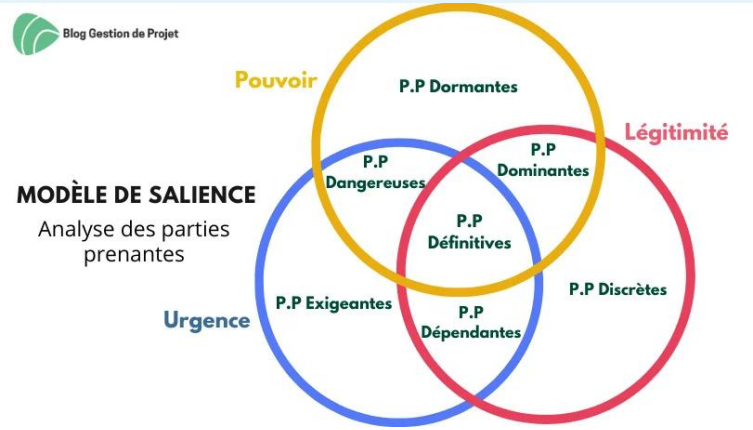
- Mise en place d’un comité cybersécurité auprès de la direction.
- Audit externe annuel de sécurité.
- Formation continue des collaborateurs.
- Politique de transparence et d’information continue envers les parties prenantes.

“Mais au fait … : qui sont mes parties prenantes ?”

Les identifier …

Les classifier … (SWOT etc.)





La supply chain, un maillon critique

La cybersécurité doit être intégrée dans l'évaluation, la contractualisation et la surveillance des partenaires.

Une entreprise ne peut être cyber-résiliente seule : c'est **tout l'écosystème** (clients, fournisseurs, sous-traitants) qui doit être aligné.

→ Les TPE-PME sont souvent les portes d'entrée des cybercriminels pour atteindre des entreprises plus grandes via leurs connexions commerciales

→ Une cyberattaque sur un tiers peut entrainer des impayés, arrêts de production, rupture des livraisons voire défaillance de plusieurs maillons.

60% des entreprises victimes d'une cyberattaque ne se relèvent pas dans les 18 mois : **effet domino** sur la supply chain

Réparer : le choc **technique**, oui… mais surtout le choc **relationnel**

	VISIBLE	INVISIBLE
	🔧 **Choc TECHNIQUE**	🤝 **Choc RELATIONNEL**
Impact	Indisponibilité des services Perte de données Coûts de restauration Mobilisation massive des équipes	Interruption de contrats clients Exfiltration d'informations sensibles Coûts de gestion de crise Perte de confiance interne et externe
Durée typique	Heures → jours	Jours → mois

Campagne massive sur les réseaux contre l'opérateur et plusieurs appels à aller chez les concurrents (SFR, Orange)

Chute brutale de l'action de 31%

Une mauvaise gestion alimente la défiance. Tout est une question d'**équilibre entre gestion du choc technique et gestion du choc relationnel**.
Clients, collaborateurs, partenaires et institutions veulent des **réponses claires**, des **preuves d'action**, et une posture **responsable**.

Gérer la confiance en 4 temps.

*Une crise bien pilotée **réduit l'impact technique** et **limite le choc relationnel** :*
*la **préparation**, la **clarté des rôles** et la **répétition des exercices** font toute la différence*

ANTICIPER : vacciner avant une attaque

Gouvernance, entraînements, contractualisation

Communication rapide, définition des niveaux d'alerte, coordination

REAGIR : contrôler pendant une attaque

TRANSFORMER : être préparé et mieux protégé

RETEX, culture cyber, résilience

Transparence, accompagnement, restauration des sauvegardes

RECONSTRUIRE : récupérer avant une attaque

ENTREPRISE = organisme qu'il faut protéger

Gérer la confiance en 4 temps.

Investir dans la communication post-attaque coûte souvent bien moins cher que les conséquences d'un silence ou d'un message mal calibré.

TRANSFORMER : être préparé et mieux protégé

Se transformer après une cyberattaque : un investissement, pas une dépense. Après une crise, peu d'entreprises prennent le temps de transformer leur posture, leur culture, leur communication. Pourtant, c'est là que se joue la vraie résilience.

	EQUIFAX (2017)	CAPITAL ONE (2019)
Personnes affectées	~147 M de données personnelles clients	~106 M de données personnelles clients
Réaction	**Annonce tardive** (environ 6 semaines après découverte), communication critiquée	**Annonce rapide**, coopération FBI, arrestation du suspect, monitoring d'identité offerte
Règlements	575 M$ - 700 M$ (FTC + États) → total **1,3 – 1,4 Md $** avec remédiation	**190 M$** par recours collectif
Impact réputation	Confiance durablement entamée, critiques parlementaires, réputation abîmée	Réputation affectée à court terme mais restaurée via communication et mesures correctives

M = million ; Md = milliard

Impact boursier des cybercrises… sur fond de guerre éco

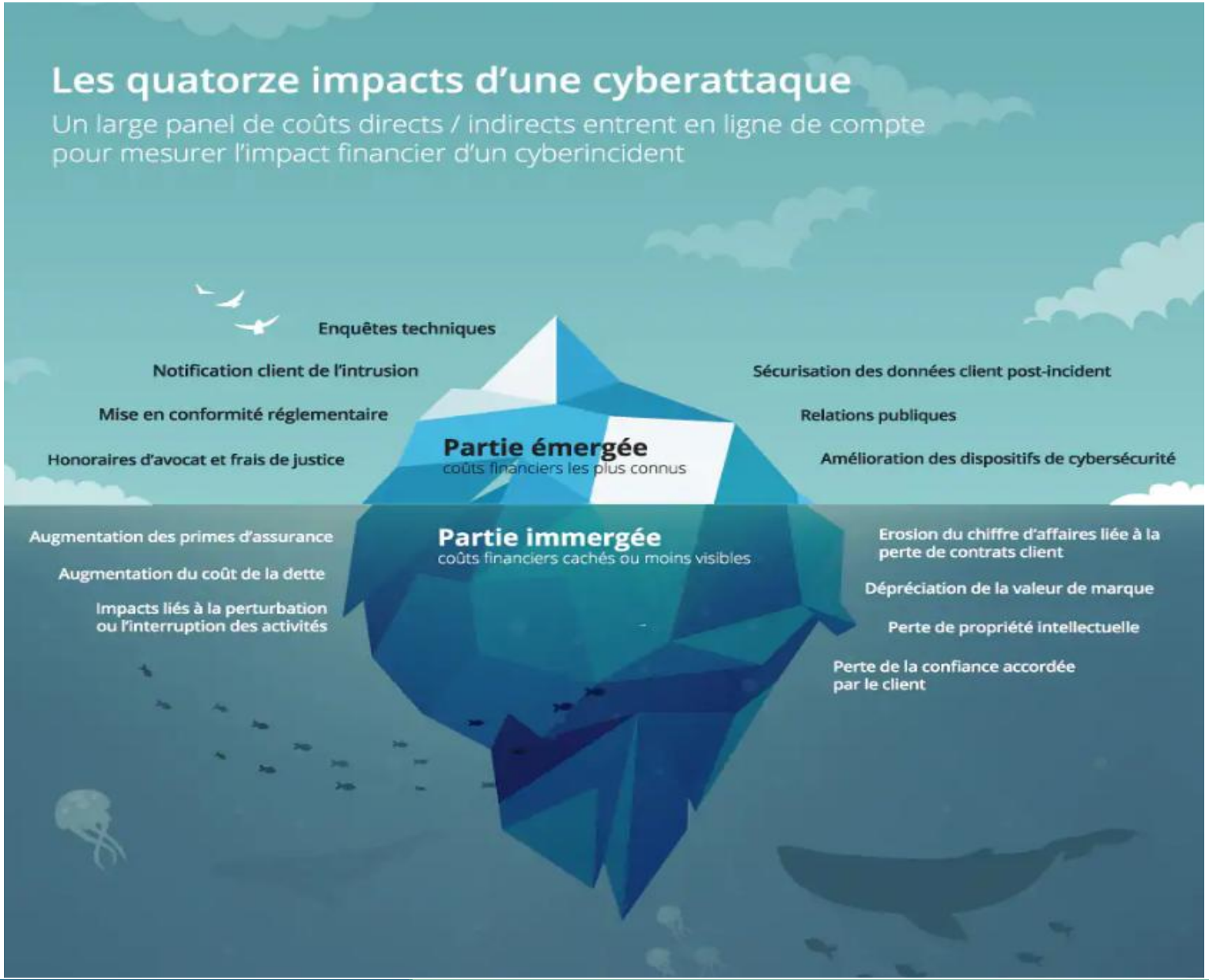
Equifax (2017) : Communication **tardive**
Après l'annonce : **-13%**
Jours suivants : **-31%** sur 10j
Long terme : retour progressif (plusieurs mois)

SolarWinds (2020) : Communication **difficile**
Après l'annonce : **-16%**
Jours suivants : **-40%** sur la semaine
Long terme : stabilisation lente (forte volatilité)

Target (2013) : Bonne communication
Après l'annonce : **-8% à -10%**
Jours suivants : stabilisation
Long terme : retour complet du cours (3 mois)

Coinbase (2025) : Bonne communication
Après l'annonce : **-6% à -7%**
Jours suivants : stabilisation partielle
Long terme : stabilisation rapide (1 à 2 mois)

Okta (2023) : Communication initiale rapide, puis révélations ultérieures
→ Après l'annonce initiale : **-11%**
→ Jours suivants : stabilisation, puis révélations provoquant une nouvelle baisse de **-5% à -7%**
→ Long terme : stabilisation et regain de confiance lents (7 à 10 mois)



En résumé

Sans oublier le 15ème … :
L'accompagnement des parties prenantes …
(réactions, e-reputation, impact, coût…)

Questions-réponses

Reprise dans 30 minutes

Table ronde 2

Leviers et solutions

Sébastien DUPENT
Pascal MARY

Grégory BUZOLICH
Colonel Frédéric AVY

EDITION 2025

Souveraineté numérique et gestion des risques : pourquoi l'identification des actifs critiques est prioritaire

Monsieur Sébastien DUPENT

Professeur agrégé en Economie et Gestion spécialité système d'information - Spécialiste cybersécurité - Lycée René Cassin
RC Gendarmerie nationale

Identifier

Cartographier les actifs critiques (données, applis, prestataires)

Prioriser

Scorer: impact x dépendance x reversibilité

Protéger

Décider: clauses, alternatives, PRA & journalisation

Pourquoi maintenant?

Trois impacts concrets

Business

arrêt de service
= perte de CA
/ production

Conformité

NIS2 - RGPD
Data Act
= obligations et
sanctions

Réputation

confiance
clients &
partenaires

L’identification comme condition préalable à la gestion des risques

Normes et cadres : ISO 27005 / NIS2

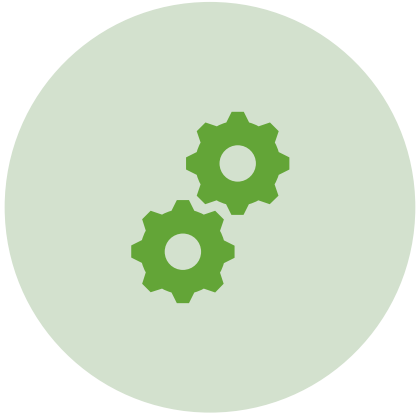
Première étape de toute démarche : **identifier les actifs**.

ISO 27005 : identification → évaluation → traitement des risques.

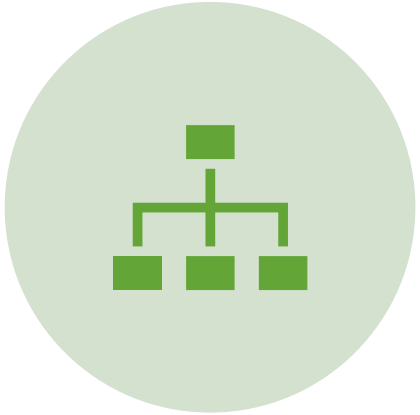
NIS2 : obligation de **documenter les dépendances critiques** et d'assurer la continuité de service.

➡️ **On ne protège que ce que l'on connaît.**

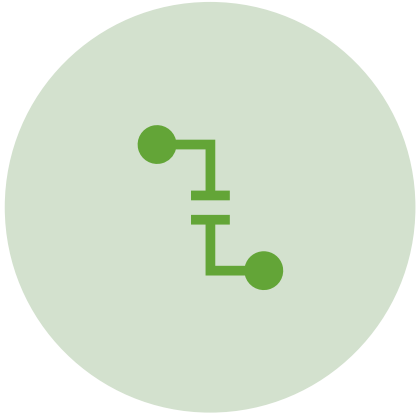
Dimensions à considérer



TECHNIQUES :
INFRASTRUCTURES, SYSTÈMES, LOGICIELS.



ORGANISATIONNELLES :
PROCESSUS MÉTIERS, DONNÉES SENSIBLES, PRESTATAIRES.



STRATÉGIQUES : DÉPENDANCES EXTERNES, FOURNISSEURS, TECHNOLOGIES.

➡️ Une approche globale reliant sécurité et gouvernance.

Outil clé : cartographie → hiérarchisation → protection

01

Cartographier : visualiser les dépendances et interconnexions.

02

Hiérarchiser : prioriser selon la criticité.

03

Protéger : sécuriser les actifs vitaux.

➡️ La sécurité devient une **stratégie proactive**.

Souveraineté numérique = d’abord identification des actifs critiques

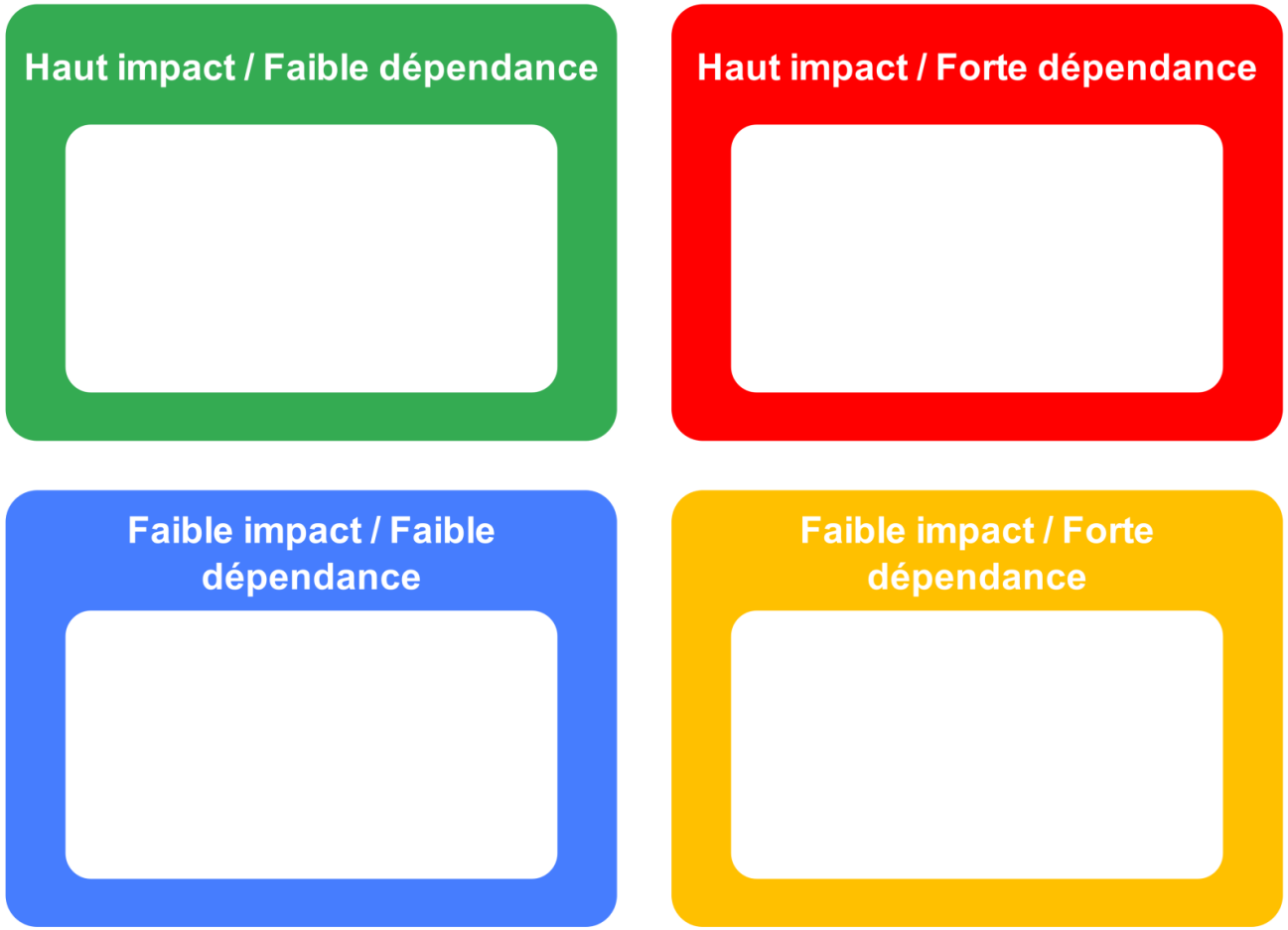
➡️ **Identifier, c’est maîtriser.**

Base pour la gestion des risques, la résilience et la coopération

- Identifier les actifs critiques, c'est :
  - cibler les efforts de **sécurité** ;
  - renforcer la **continuité d'activité** ;
  - faciliter la **coopération entre acteurs publics et privés**.

➡️ Une approche commune de la sécurité numérique.

Matrice Impact × Dépendance

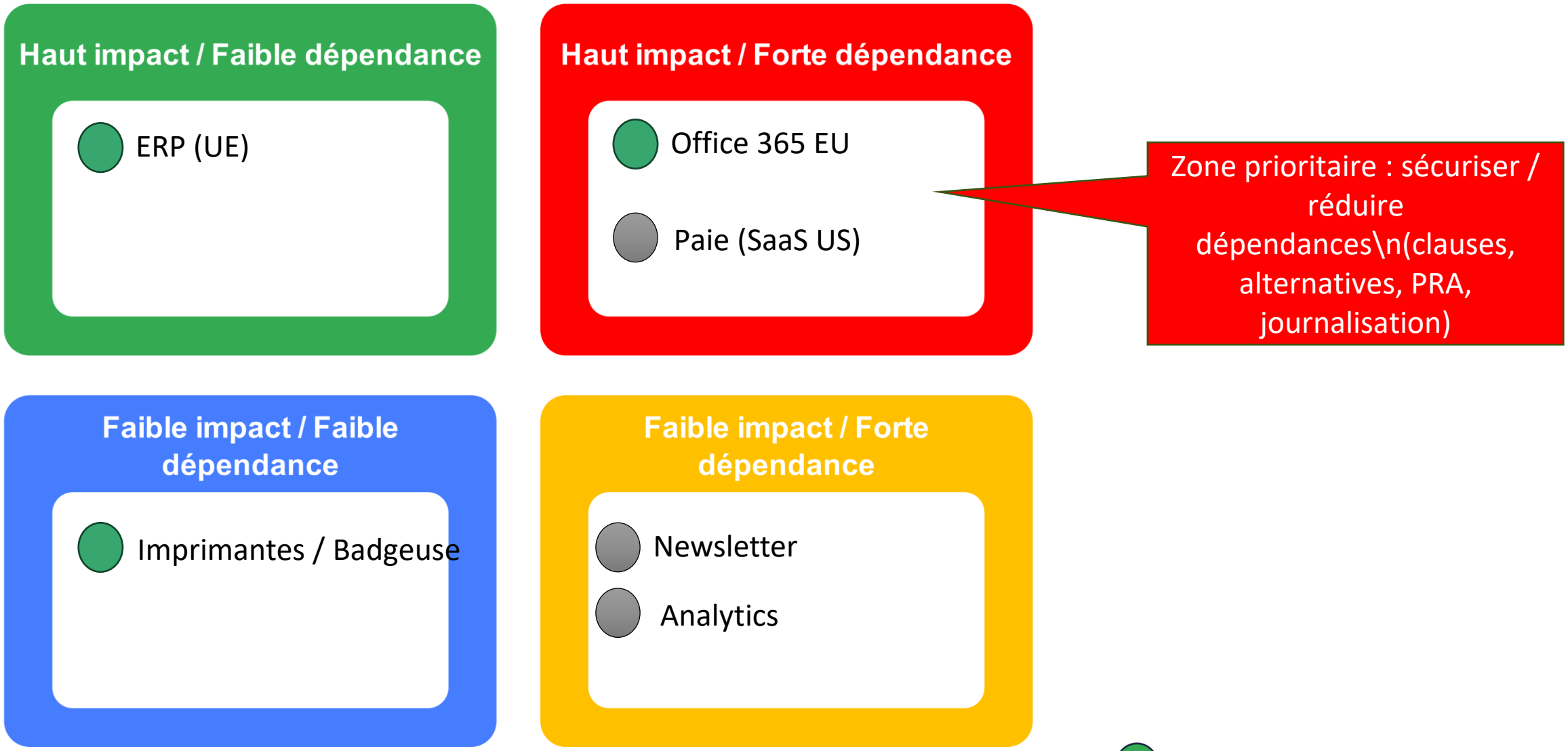


- Encodez la couleur : UE (vert) / hors-UE (gris) pour visualiser la souveraineté.
- Quadrant en haut à droite = Priorités N°1 (actions 0–90 j).
- Placez vos services/applications (post-it par actif).

Actif hébergé/opéré en UE (souverain)

Actif hors UE / dépendance extra-UE

Matrice Impact × Dépendance



Zone prioritaire: 4 leviers concrets

Localisation des données et sous-traitants (UE vs hors UE)

Réversibilité & formats d'export ouverts (frequence d'export)

Altematives / POC de secours (plan B réaliste)

PRA testé journalisation (preuve et traçabilité)

Plan d'exécution en 90 jours

Objectif : visibilité partagée, premières décisions, premières remédiations.

J+61 → J+90 : Décider & exécuter

- Valider feuille de route 6–12 mois au COMEX/Direction
- Lancer 3–5 mesures à impact rapide (journalisation, MFA, PRA ciblés)
- Clauses contractuelles & exigences fournisseurs
- Plan de tests (restauration, continuité, exercices)

J+31 → J+60 : Cartographier & prioriser

- Carto dépendances (UE / hors-UE, contrats, clauses)
- Matrice Impact × Dépendance (atelier de priorisation)
- Identifier les mesures à impact rapide & mesures transitoires
- Préparer décisions (budget, arbitrages, clauses)

J+0 → J+30 : Cadrer & démarrer

- Nommer pilote + Autorité de validation, définir le périmètre
- Atelier par service pour remplir la checklist
- Inventaire initial (actifs, fournisseurs, données)
- Risques majeurs connus, dettes techniques visibles

RACI(matrice des rôles) minimal : Autorité de validation (décision), Pilote (coordination), Métiers (inputs), RSSI/Conformité (exigences), Achats/Legal (contrats).

Construire une cartographie commune et transfrontalière

- Les flux numériques ne s’arrêtent pas aux frontières.
  - Créer une **cartographie partagée** permet de mieux prévenir, réagir et protéger.

➡️ Vers une **autonomie numérique européenne collective**.

Exiger plus de vos fournisseurs pour risquer moins

Monsieur Pascal MARY

Head of Cybersecurity and Data Protection - Hager Group
RC Gendarmerie nationale

Pourquoi vérifier ses fournisseurs ?

Les **dépendances numériques augmentent la surface d'attaque** et compliquent la détection.

Les tiers (fournisseurs, sous-traitants, éditeurs) sont **des points d'entrée** privilégiés.

60% des cyberattaques exploitent aujourd'hui les vulnérabilités de la chaine d'approvisionnement.

- **> Obligations légales en vigueur ou à venir … et autres normes :**

NIS 2 (EE et EI) - CRA (IoT) - RGPD (art 28) – DORA (banques) – LPM (OIV/OSE) – PCI-DSS (paiement en ligne) - ISO 27001 (normes) - ECOVADIS (performances RSE)

Mécanismes d'une attaque Supply Chain

Principe : une attaque sur un fournisseur ou partenaire qui sert de tremplin vers la cible principale.

- **Fournisseur de logiciels compromis** → diffusion d'un code malveillant.
- **Sous-traitant industriel infecté** → accès indirect au réseau du client.
- **Prestataire de maintenance négligent** → vol d'identifiants ou sabotage.

🎯 Cible finale : systèmes de production, données clients, R&D….

JAGUAR
LAND ROVER
NAVAL GROUP
solarwinds

Comment faire ? 3 étapes

Chef de projet

Fournisseur

RSSI

Resp Achat.

1 - Evaluer

- **Lister les fournisseurs** critiques (*digitaux et stratégiques*)
- Envoyer un **questionnaire** simple qui standardise les réponses (vert – jaune – rouge) + demande de preuves (**maxi 25 questions**)
- **Evaluer les risques** (*via des critères standards et simple*) sur la base des réponses obtenues

2 - Aligner

- **Organiser une revue** tripartite (RSSI, chef de projet, fournisseur)
- Etablir un **plan de remédiation** conjointement

3 - Contractualiser

- **Annexer le plan de remédiation** et les engagements
- **Contrôler** la mise en application des mesures
- **Réviser** régulièrement en fonction du contexte

Oui à un formulaire, non à la bureaucratie

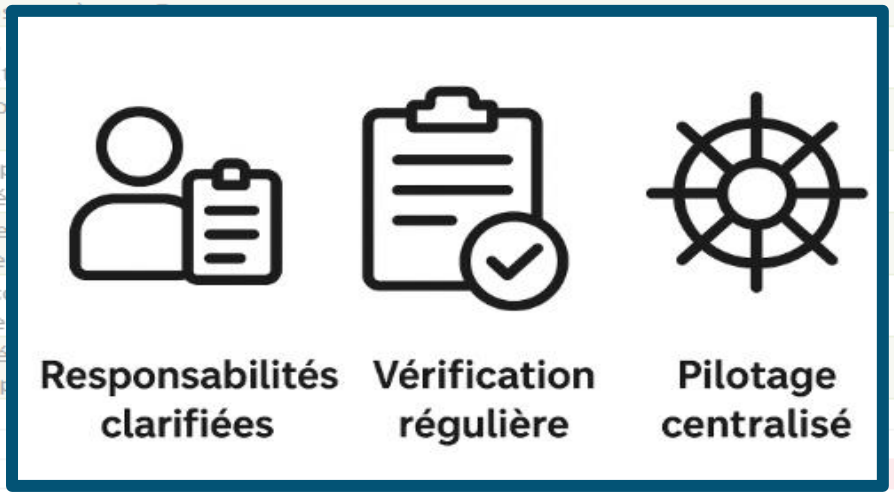
Grille d'évaluation de la posture de sécurité du fournisseur

Domaine	Question experte	Question simple	Score (1=Faible, 2=Moyen, 3=Fort
Gouverna	Disposez-vous d'un cadre de gouvernance de la sécurité de	Avez-vous des règles écrites qui expliquent nt vous protégez les informations ?	
Gouverna		anisme externe vérifie-t-il régulièrement écurité ?	
		nt vous assurez-vous que vos prestataires	
Protectio			
Protection des données	restauration ?	de vos données, et les testez-vous ?	
Protection des données	Êtes-vous en conformité avec le RGPD ?	Respectez-vous les règles de protection des données personnelles ?	
Sécurité opérationnelle	Disposez-vous d'un processus de gestion des correctifs et vulnérabilités ?	Vérifiez-vous et corrigez-vous régulièrement les failles dans vo	
Sécurité opérationnelle	Quels mécanismes de défense périmétrique et de détection d'intrusion utilisez-vous ?	Avez-vous des détecter les at	
Sécurité opérationnelle	Réalisez-vous des tests de sécurité applicative (SAST/DAST, pentests) ?	Vos logiciels so sécurité ?	
Gestion d		ous un p e donné	
Gestion des incidents	leurs données ?	bien de quelque chose	
Continuité & résilience	Disposez-vous d'un plan de continuité et de reprise d'activité testé régulièrement ?	Pouvez-vous c gros problème	
Continuité & résilience	Où sont hébergées les données (UE / hors UE), et sous quelles garanties contractuelles ?	Où sont stocké lois elles sont p	
		Score total	0
		Niveau global	

Simplicité et précision vont de pair :

Question experte	Question simple
Utilisez-vous une authentification multifactorielle (MFA) pour les accès sensibles ?	Demandez-vous une double vérification (comme un code sur le téléphone) pour se connecter ?

La vérification renforce la confiance :



Conclusion :

A SAVOIR*

88 % des entreprises jugent **le risque fournisseurs « très important » ou « important ».**

Seules **33,6 % des entreprises évaluent tous leurs fournisseurs.**

Près de **la moitié** (47 %) des entreprises engagées **effectuent une révision chaque année.**

Exiger plus de vos fournisseurs, c'est risquer moins, ….
mais c'est aussi construire des partenariats plus solides et plus durables !

**source : CESIN x Board of Cyber : Observatoire 2024 Le risque cyber lié aux fournisseurs – 06/12/2024*

Compétences & culture de souveraineté

Monsieur Grégory BUZOLICH

Directeur des Ressources Humaines – ALSACHIMIE
Magistrat – Conseil de Prud'homme de Mulhouse
RC Gendarmerie nationale

Compétences et culture de souveraineté

- Quelques pistes pour développer une conscience de souveraineté
  - En entreprise notamment dans le domaine TI
  - Participer au développement d'une souveraineté française dans le domaine cyber
- Vérifier, clarifier et garantir les Pré-requis
  - **Volonté**
  - **Cohérence**
  - Objectifs
  - Priorités

Compétences et culture de souveraineté

- Se préparer en définissant une politique stratégique
  - Donner du sens
  - Identifier les obstacles et les défis auxquels se préparer
  - Veiller aux 6 règles stratégiques

Compétences et culture de souveraineté

- Clarifier les moyens engagés
  - Ressources Budgétaires
  - Ressources Matérielles
  - Ressources Humaines internes ou externes
  - Ressources intellectuelles & techniques

Compétences et culture de souveraineté

- Engager un processus de conduite du changement
  - **La Répétition** fixe la notion (Drill)
    - Communication, Formation, Sensibilisations et interventions extérieures (Cyber-Gend)
  - Structurer des **Contraintes et une dynamique participative**
    - Chartes, règlement intérieur, Groupe de Travail participatif
  - Quand survient la **Crise**
    - Trop tard, échec … ou opportunité(s) à saisir

Compétences et culture de souveraineté

- En conclusion
  - Avoir la Volonté
  - Définir une Stratégie
  - Allouer des Moyens
  - Impulser et accompagner le changement

La lutte contre la cybercriminalité : le rôle du ministère de l'Intérieur

Colonel Frédéric AVY

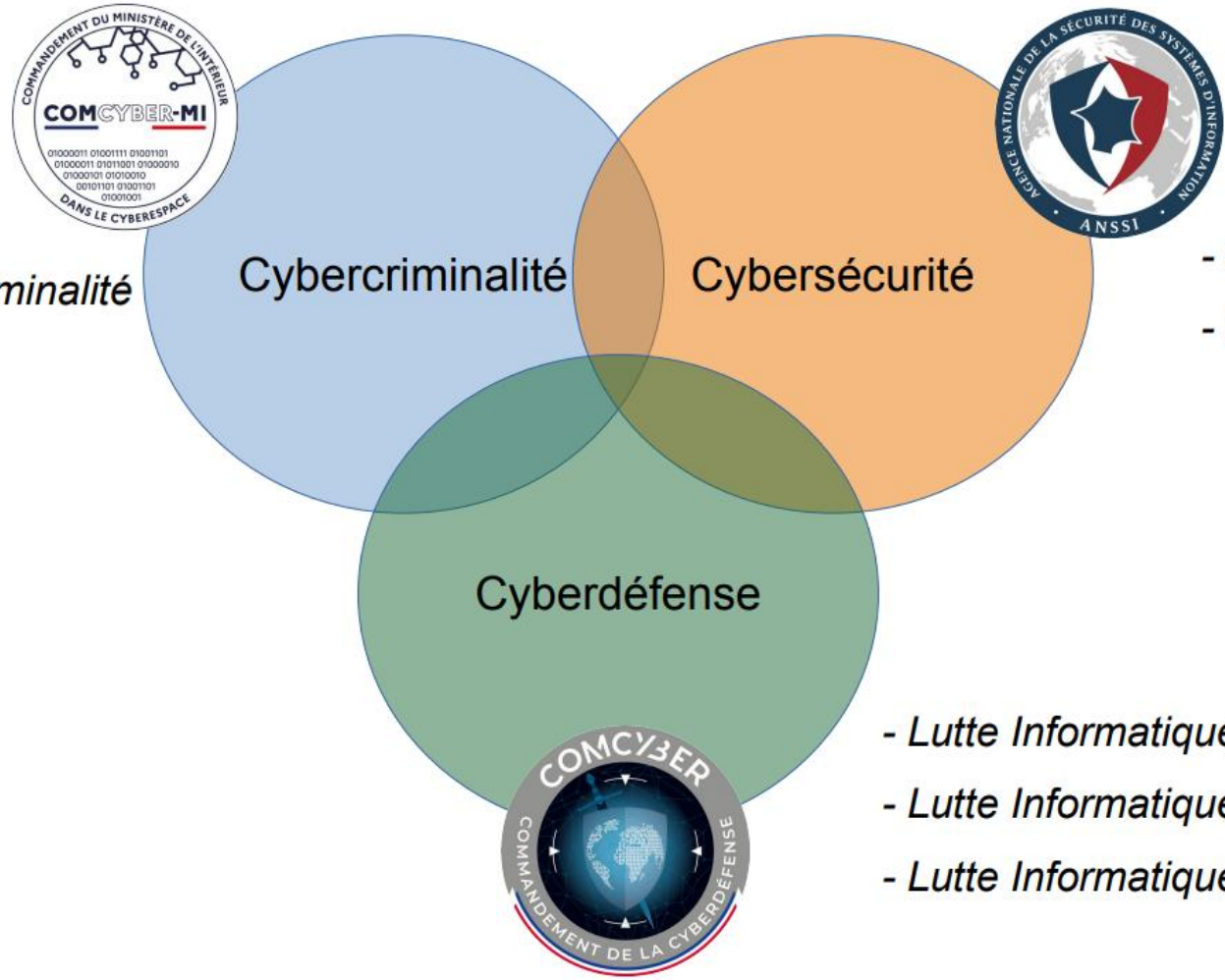
Chef de la division Stratégie, Commandement du ministère de l'Intérieur dans le cyberespace

COMCYBER-MI

« Nos forces, pour votre cyber-protection »

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Vocabulaire et périmètres d'action



- *Lutte contre la cybercriminalité*

- *Sécurité réseaux et SI*
- *Réponse aux incidents*

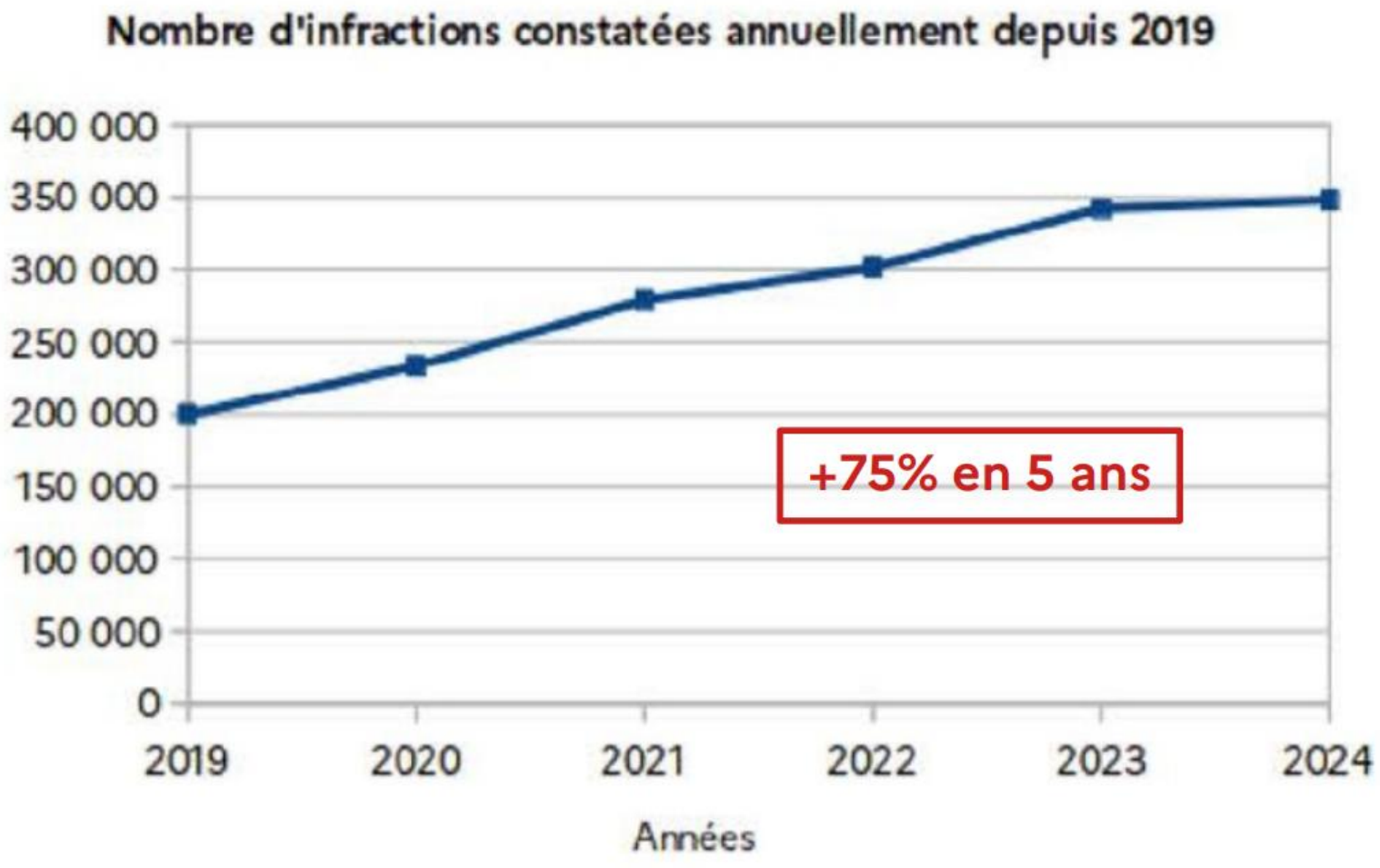
- *Lutte Informatique Défensive*
- *Lutte Informatique Offensive*
- *Lutte Informatique d'Influence*

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

État de la menace

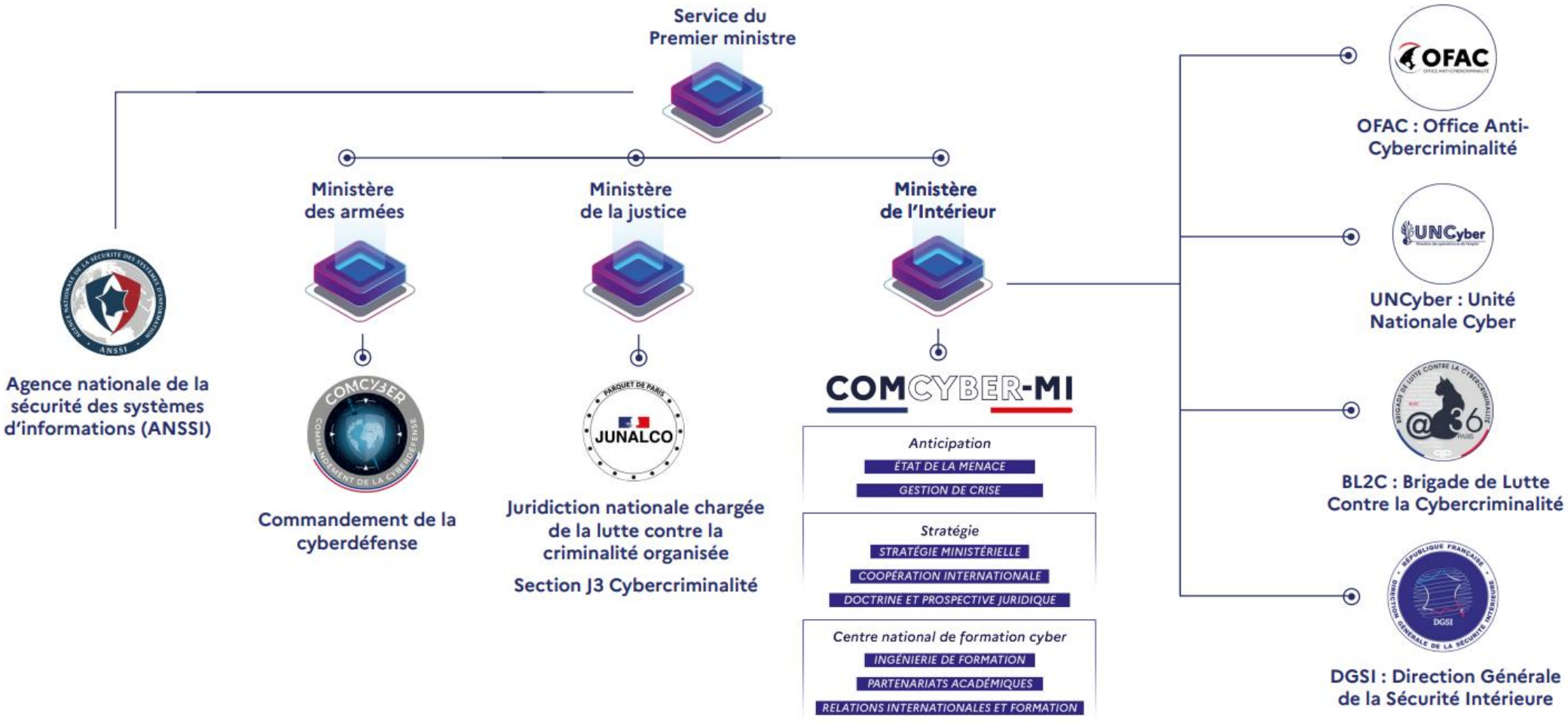
348 000

atteintes numériques
enregistrées en 2024



MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Écosystème étatique de lutte contre la cybercriminalité



MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

COMMANDEMENT DU MINISTÈRE DE L'INTÉRIEUR
COMCYBER-MI
DANS LE CYBERESPACE

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

L'action inter-administrations du COMCYBER-MI en matière de formation

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

L'action internationale du COMCYBER-MI en matière de formation

MINISTÈRE
DE L'INTÉRIEUR
*Liberté
Égalité
Fraternité*

L'accompagnement

Se renseigner

CYBERMALVEILLANCE.GOUV.FR

- *Prévenir et sensibiliser les internautes sur la cybercriminalité.*
- *Participe à la sécurisation des systèmes d'information des organisations.*

SecNum académie

- *Être sensibilisé à la sécurité numérique (MOOC).*

CSIRT RÉGIONAUX

- *Des centres régionaux pour vous aider à trouver des prestataires proches de chez vous.*

Construire sa sécurité cyber

- *Des guides pour renforcer son système d'information et se préparer à une crise cyber.*
- *Connaître et déployer les bonnes pratiques. Signaler des vulnérabilités.*

MonAideCyber
INNOVATION ANSSI

- *Un service gratuit de diagnostic cyber rapide, réalisé par des tiers de confiance, pour développer la maturité cyber des organisations.*

CNIL.

- *Comprendre ses obligations légales. Des outils à disposition pour aider à protéger les données à caractère personnel.*
- *Se renseigner sur les données personnelles, l'exercice de ses droits ou faire un MOOC sur le RGPD.*

VOUS AVEZ UN DOUTE SUR UN E-MAIL ?

Signalez-le comme spam sur la plateforme :

signal spam

Réagir face à des atteintes numériques

MINISTÈRE DE L'INTÉRIEUR ET DES OUTRE-MER — 17 CYBER — Cybermalveillance.gouv.fr

- *Assister les victimes d'atteintes numériques.*

CSIRT RÉGIONAUX

- *Apporter des conseils et aider à trouver des prestataires.*

CNIL.

- *Prévenir en cas de fuite de données personnelles, réelle ou supposée.*

- *Assister les entités essentielles et les entités importantes ou intervenir pour des faits très sensibles.*

https://www.cybermalveillance.gouv.fr/gestion-de-crise/sency-crise

ALERTE | Violation de données personnelles Free : situation, risques et recommandations

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

ESPACE PRESTATAIRE | MON ESPACE

LES MENACES ET BONNES PRATIQUES | L'ACTUALITÉ DE LA CYBERMALVEILLANCE | NOUS DÉCOUVRIR | VICTIME D'UN ACTE DE CYBERMALVEILLANCE ?

BIENVENUE DANS SENCY-CRISE

Initiation à la gestion de crise cyber pour les petites et moyennes structures

Les experts en gestion de crise cyber du Comcyber-MI appuyés par les réservistes de la gendarmerie nationale se sont associés à Cybermalveillance.gouv.fr pour accompagner les petites et moyennes entreprises, associations et collectivités à faire face aux cyberattaques.
Ce MOOC comprend des outils et conseils simples à mettre en oeuvre pour mettre en place ou améliorer le dispositif de gestion de crise cyber au sein de votre organisation.

Sen Cy-Crise
Initiation à la gestion de crise cyber

32min

Avant la crise - Anticiper pour mieux se préparer

- Se connaître
- S'informer
- Se préparer

COMMENCER →

69min

Pendant la crise - Faire preuve de résilience

- Qualifier la crise
- Alerter
- Gérer la crise
- Paroles d'experts

COMMENCER →

22min

Après la crise - Capitaliser pour mieux anticiper

- Capitaliser sur la crise
- S'exercer et s'entrainer

COMMENCER →

Ensemble, préparons-nous à affronter la crise cyber

Plus qu'une initiation à la gestion de crise cyber, SenCy-Crise est une invitation à agir, à renforcer vos défenses et à collaborer pour un avenir numérique plus sûr.

Sen Cy-Crise
Initiation à la gestion de crise cyber

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

MonAideCyber
INNOVATION ANSSI

La Suite cyber | S'inscrire | Se connecter

monaide.cyber.gouv.fr

Accueil | Les Aidants cyber | Promouvoir | Votre diagnostic cyber gratuit

MonAideCyber

Des Aidants cyber mobilisés pour aider les entités publiques et privées à prendre leur cyberdépart !

Devenir Aidant cyber | Bénéficier d'un diagnostic cyber

Un dispositif étatique

MonAideCyber est proposé par l'Agence nationale de la sécurité des systèmes d'information.

Une communauté de confiance

Les Aidants cyber sont issus de la sphère publique ou sont membres d'associations œuvrant pour un numérique de confiance.

Au service de l'intérêt général

Le diagnostic cyber aide les entités qui souhaitent se protéger contre les cyberattaques et passer à l'action.

Centre d'aide

https://17cyber.gouv.fr

17 CYBER

Mon assistance en ligne

Victime de cybermalveillance ? Nous vous guidons pour agir.

Un service proposé par la Police Nationale, la Gendarmerie Nationale et Cybermalveillance.gouv.fr

Faire le diagnostic de votre situation

Vous avez besoin d'aide pour identifier votre problème ?

Répondez à quelques questions pour déterminer l'attaque dont vous êtes victime.

Démarrer le diagnostic

Vous connaissez déjà votre problème?

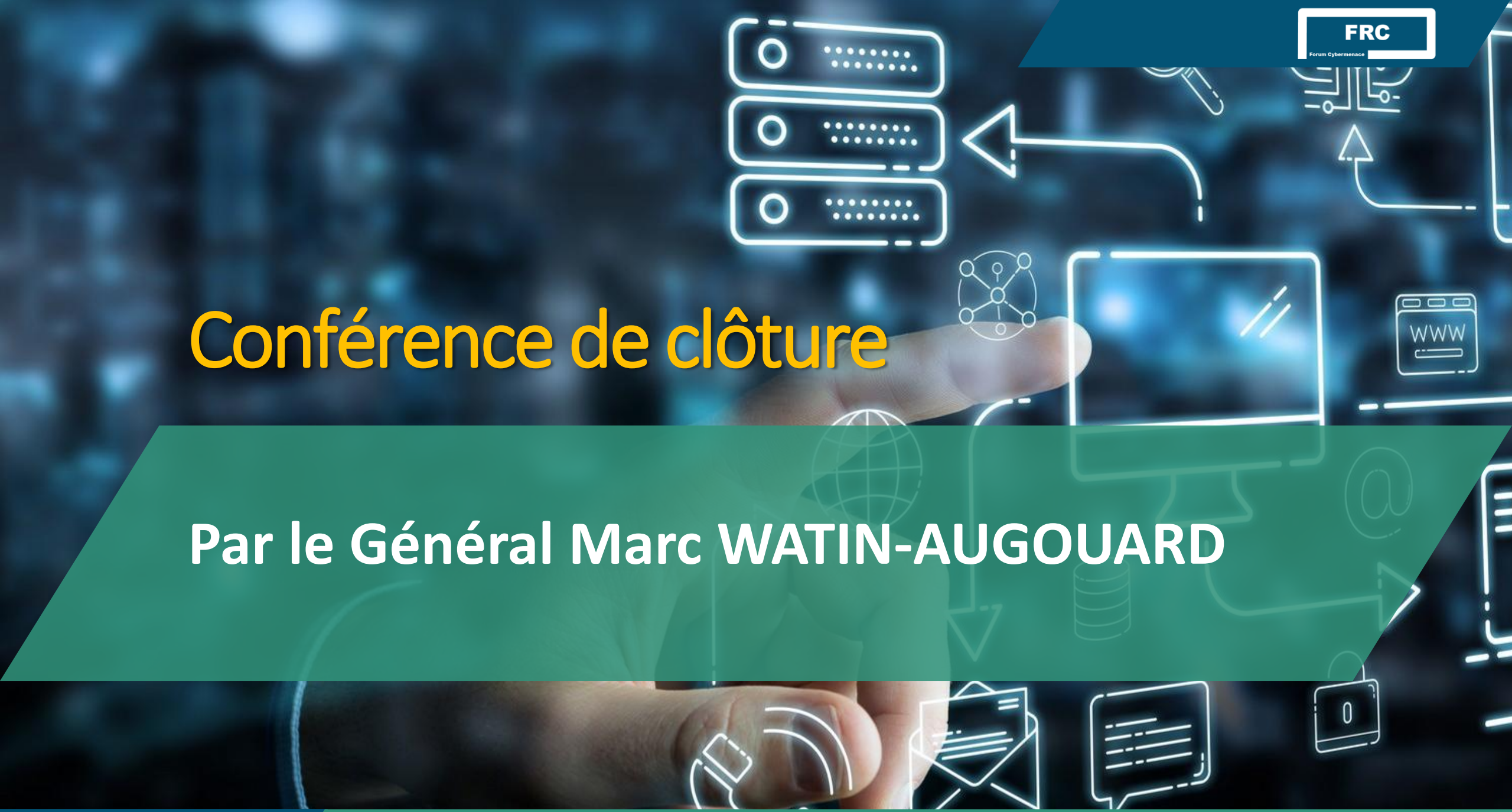
Consultez nos recommandations pour votre problème (ex : hameçonnage, piratage, virus informatique etc.)

Voir les recommandations

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Questions-réponses

Nos observateurs spéciaux …



Conférence de clôture

Par le Général Marc WATIN-AUGOUARD

EDITION 2025

Général d'armée (2s)
Marc WATIN-AUGOUARD

Fondateur du Forum International de la Cybersécurité
InCyber (FIC) - Europe

Générale de corps d'armée Florence GUILLAUME

Commandant la région de gendarmerie du Grand Est, commandant la gendarmerie pour la zone de défense et de sécurité Est

Général Gwendal DURAND

Commandant le Groupement de Gendarmerie Départementale du Bas-Rhin

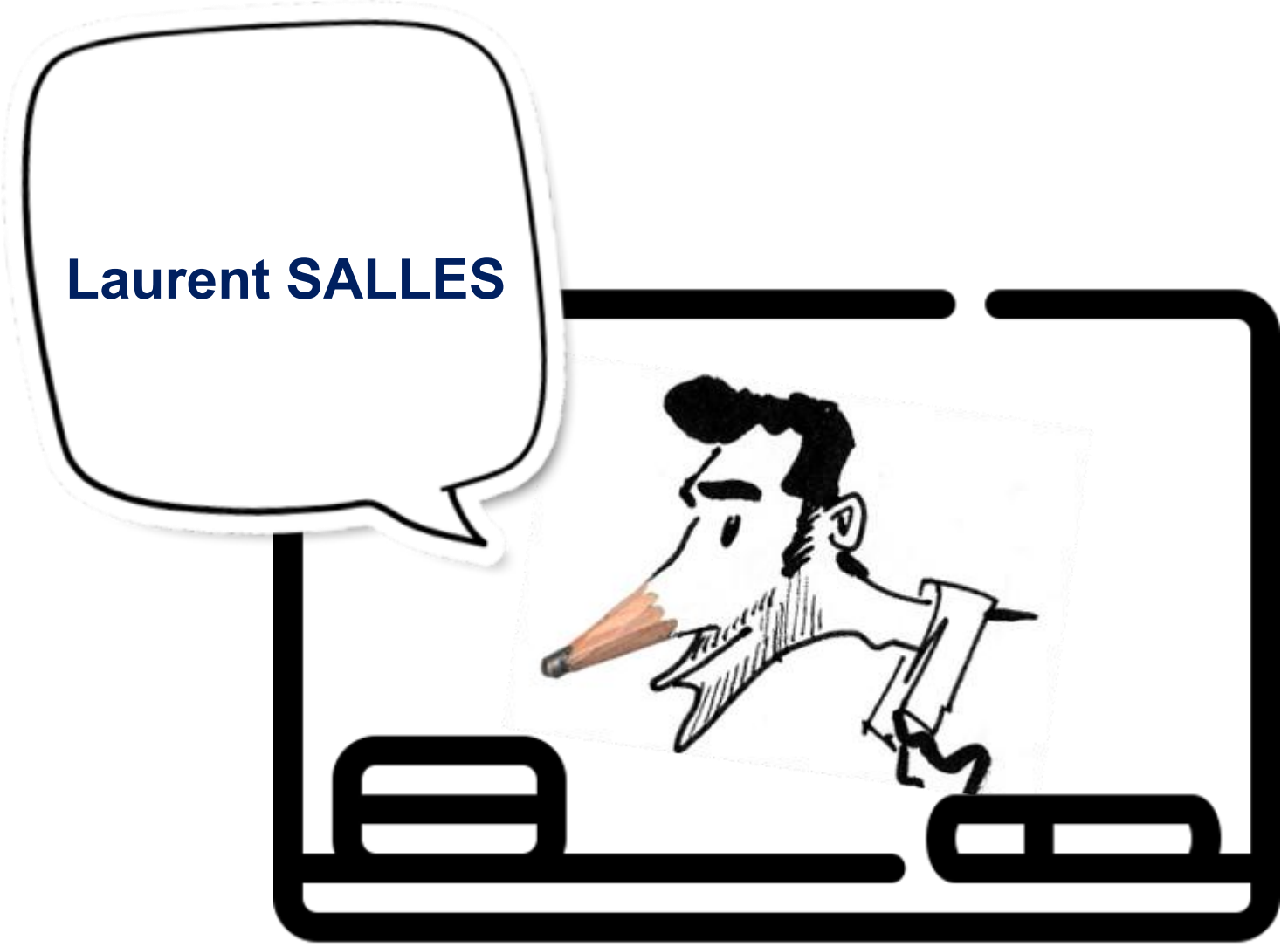
Monsieur Gilbert GOZLAN

Président Ad honores - Réseau Alsace
RC Gendarmerie Nationale

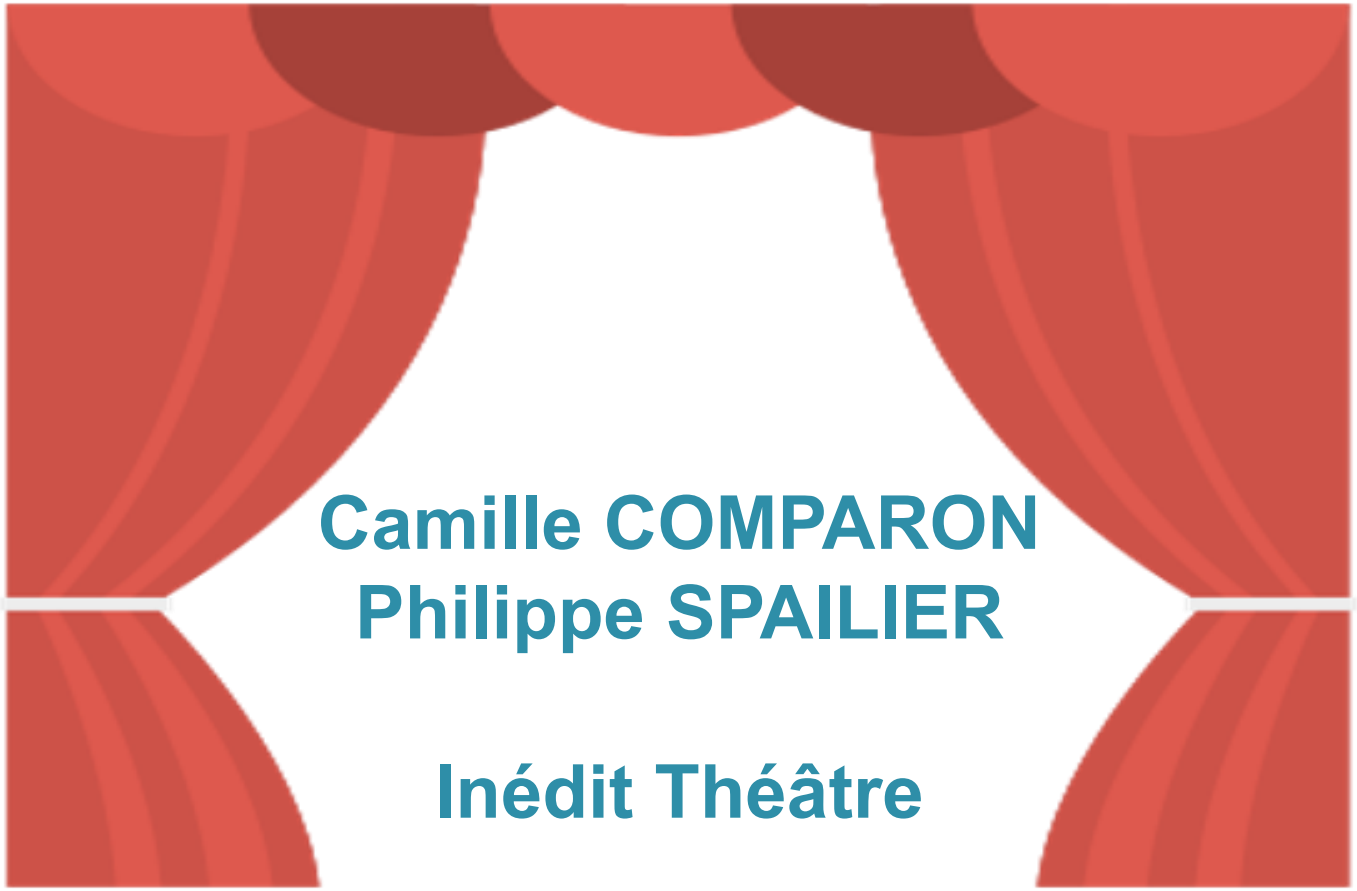
Remerciements

MDL Vanessa BOTRA
Grégory BUZOLICH
Anthony CHARREAU
Sébastien DUPENT
Régis ECKART
Damien ERNST
Gilbert GOZLAN
MDC (RO) Carole GIRAUD
Emmanuelle HAASER
Ludovic HAYE
Hervé HUMBERT
Pascal MARY
Sophie MARTIN
Didier SCHERRER
ADJ Sébastien STOUFFLET
Elena VALLEJO
Jonathan WEBER

Remerciements



Remerciements



Questionnaire de satisfaction

Flashez ce QR Code

Donnez votre
avis sur le
18e FRC

Prochain Forum Incyber Europe

Rendez-vous au prochain Forum du Rhin supérieur sur les Cybermenaces

Mardi 3 novembre 2026

19e FRC

https://adhonores.alsace/

Questionnaire de satisfaction

Flashez ce QR Code

Donnez votre
avis sur le
18e FRC