

# FORUM DU RHIN SUPERIEUR SUR LES CYBERMENACES

16ème édition - INSP Strasbourg

**Cybermenaces subtiles**  
**S'engager pour ne pas subir**

# Madame Emmanuelle HAASER

Responsable veille et marketing - CCI Alsace Eurométropole  
Lieutenant-colonel (RC) de la Gendarmerie Nationale

# Monsieur Frédéric FESSAN

Secrétaire général

Institut National du Service Public - INSP

## Général Jude VINOT

Commandant le Groupement de Gendarmerie Départementale du Bas-Rhin

# Monsieur Jean-Luc HEIMBURGER

Président de la CCI Alsace Eurométropole

## Madame Irène WEISS

Conseillère régionale déléguée à la cybersécurité

Vice-présidente de la commission Enseignement supérieur, Recherche et Innovation

## CYBERMENACES SUBTILES S'engager pour ne pas subir

### 7 NOVEMBRE 2023

auditorium de l'INSP  
1 rue Sainte Marguerite à Strasbourg

FRC

16ème édition

13H00 OUVERTURE DES PORTES

13H30 DISCOURS D'OUVERTURE

**Général Jude VINOT** - Commandant le Groupement de Gendarmerie Départementale du Bas-Rhin

**Jean-Luc HEIMBURGER** - Président de la CCI Alsace Eurométropole

**Franck LEROY** - Président de la Région Grand Est

**Josiane CHEVALIER** - Préfète de la Région Grand Est - Préfète du Bas-Rhin

**Emmanuelle HAASER** - animation - LCL (RC) Gendarmerie Nationale

14H00 CONFÉRENCE PLÉNIÈRE

### Etat des lieux des cyberattaques en France

**Lieutenant-colonel Jean-François LALOYER** - Chef de division adjoint de la proximité numérique – ComCyberGend

14H30 TABLE RONDE # 1 : CONNAISSANCE DE L'INVISIBLE

### Au cœur d'une cyberattaque : les étapes

**Adjudante Elena VALLEJO** - Enquêtrice Cyber Fintech de la Section de Recherches de Strasbourg

**Sébastien DUPENT** - Professeur agrégé en Economie et Gestion spécialité système d'information  
Lycée René Cassin - LTL (RC) Gendarmerie Nationale

Avec la participation des étudiants en BTS SIO option SLAM 2ème année du lycée Renée Cassin.

### Présentation du centre d'assistance de proximité Grand Est Cybersécurité

**Jean-Charles RENAUDIN** - Responsable Cybersécurité & CSIRT à GRAND E-NOV+

### Dépôt de plainte, constitution du dossier

**Audrey GERBAUD** - Substitut du Procureur de la République près le tribunal judiciaire de Paris –  
JIRS/JUNALCO section cybercriminalité

### Réponse à incident/remédiation - redémarrage

**Pierre VEUTIN** - Directeur général - Soteria Lab

15H45 PAUSE

16H15 TABLE RONDE # 2 : MOBILISATION ET ACTIONS

### Evaluation des risques cyber par une méthode pratique

**Sébastien DUPENT** - Professeur agrégé en Economie et Gestion spécialité système d'information  
Lycée René Cassin – LTL (RC) Gendarmerie Nationale

### Mise en place d'actions concrètes liées à la protection des données - RGPD

**Sélim-Alexandre ARRAD** - Délégué à la Protection des Données DPD - Sénat

### Facteur humain et engagement des collaborateurs

**Marion PIERRE** - Responsable Documentaire, Data et Propriété Intellectuelle – Butachimie

**Denis MATHIS** - Responsable Hygiène Sécurité Inspection – Butachimie

17H45 CONFÉRENCE DE CLÔTURE

### Prospective : Intelligence Artificielle, cybersécurité versus cybercriminalité

**Daniel GUINIER** - Expert judiciaire honoraire  
Anc. expert devant la CPI de la Haye - COL (RC) Gendarmerie Nationale

18H30 COCKTAIL

entrée libre  
demande d'inscription sur  
[www.adhonores.alsace](http://www.adhonores.alsace)  
formulaire en ligne



# INSP

Institut national  
du service public





**CCI ALSACE  
EUROMÉTROPOLE**







**BANQUE POPULAIRE**  
ALSACE LORRAINE CHAMPAGNE







GRAND  
EST



BANQUE FRANÇAISE  
MUTUALISTE

LA BANQUE DE CHAQUE AGENT DU SECTEUR PUBLIC



#Cybersecurity

#Virtualization

#AI




## Les Gendarmeries, la RCDS et Ad honores - Réseau Alsace



# Notre objectif

« Faire connaître et partager »  
« Progresser dans les actions à mettre en œuvre pour toujours mieux impliquer l'ensemble des collaborateurs »



## FORUM DU RHIN SUPERIEUR SUR LES CYBERMENACES

LA GENDARMERIE ET LES OFFICIERS DE LA RESERVE CITOYENNE

Prénom : \_\_\_\_\_ Nom : \_\_\_\_\_

Fonction : \_\_\_\_\_ Entreprise : \_\_\_\_\_

---

**Accueil**

Je suis satisfait des conditions d'accueil au forum :      ++    +    -    --

**Table ronde « Meilleures pratiques de la cyber »**

Ce sujet est utile à l'exercice de mon métier :              

J'ai trouvé réponse à mes questions :              

**Table ronde « La sécurité du site Internet de l'entreprise »**

Ce sujet est utile à l'exercice de mon métier :              

J'ai trouvé réponse à mes questions :              

**Bilan**

Je suis globalement satisfait de ce forum sur les cybermenaces :              

Ce forum a répondu à mes attentes :              

Je conseillerai ce forum à mon entourage :              

J'ai participé au forum l'année dernière ?      oui    non

Si oui j'ai mis en place une (des) action(s) de prévention de mon entreprise ?      oui    non

Lesquelles ? .....

Je souhaite voir naître ou l'année prochaine 2022 la(s) théme(s) suivant(s) :

.....

.....

.....

Afin de garantir ce document complété de votre service de la sécurité, les informations demandées sont à destination exclusive de l'équipe de l'organisation du forum.



Connexion au réseau Wifi : WIFI\_INSP

Identifiant : **gendarmes**

Mot de passe : **P2aP2a67**

Profil : **EVENEMENT**

Dans le respect de la charte informatique de l'INSP

Conférence plénière

# Etat des lieux des cyberattaques en France

Par le lieutenant-colonel Jean-François LALOYER



# UN ÉCOSYSTÈME CYBERCRIMINEL PLUS SOPHISTIQUÉ ET PROFESSIONNEL

## Une menace sérieuse...



Actions de sensibilisation en 2022 (élus, collectivités, établissements publics, etc)



1 plainte / 250 faits tentés ou commis



**600** enquêtes  
en 2022 par la section J3  
80% sont des escroqueries (ZGN)



**2 Md€**  
**coût cyberdélinquance**  
en France (après plaintes)  
6 000 Md€ dans le monde

## ...trop peu prise en compte

Une menace numérique infinie, rapide, protéiforme, internationale et... dangereuse pour la stabilité démocratique

**+ de 50**  
vulnérabilités découvertes / jour

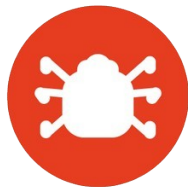
Des systèmes d'information interconnectés

**1/3** des collectivités territoriales victimes de cyberattaque en a bénéficié



## 15 MENACES

1

**Logiciel malveillant**

2

**Attaque internet directe**

3

**Hameçonnage**

4

**Attaque via une application**

5

**Courrier indésirable**

6

**Déni de service**

7

**Usurpation d'identité**

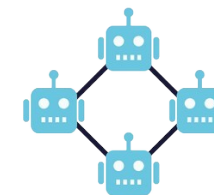
8

**Violation de données**

9

**Menace interne**

10

**Réseau de robots**

11

**Atteinte physique**  
*(dégâts, vol, perte)*

12

**Révélation d'information**

13

**Rançongiciel**

14

**Cyber espionnage**

15

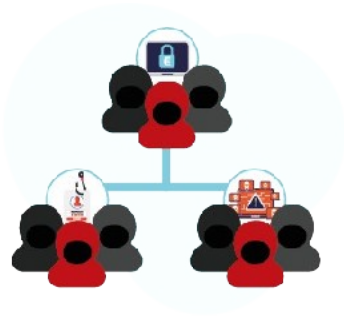
**Minage frauduleux de cryptomonnaie**

24

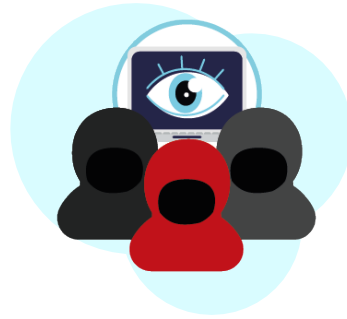




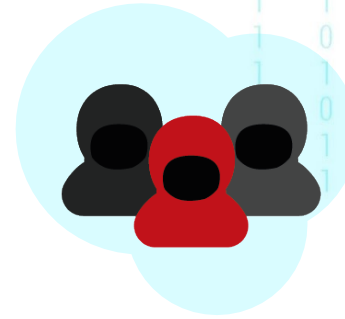
## PROFIL DES CYBERDÉLINQUANTS OBSERVÉS



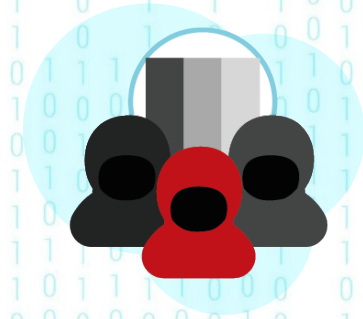
Groupes structurés et autonomes (*rançongiciels, botnets, vol de données, Caas, ...*)



Réseaux d'opportunistes (*pédocriminalité, commerces illicites,...*)



Groupes d'activistes en ligne (*manipulation de l'information, espionnage,...*)



Groupes dépendant d'un état étranger (*volonté de déstabilisation*)



Escroqueries

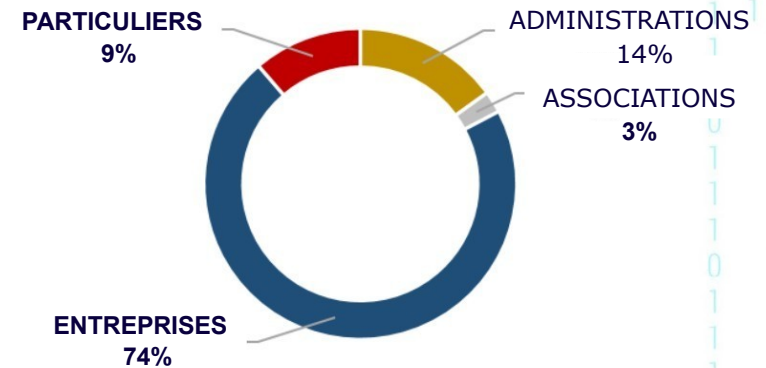


Haine en ligne et atteintes aux personnes



Atteintes aux systèmes d'informations

Répartition des victimes de rançongiciels en 2022 (source : rapport d'analyse des cybermenaces 2023)





# ANTICIPER ET SAVOIR RÉAGIR

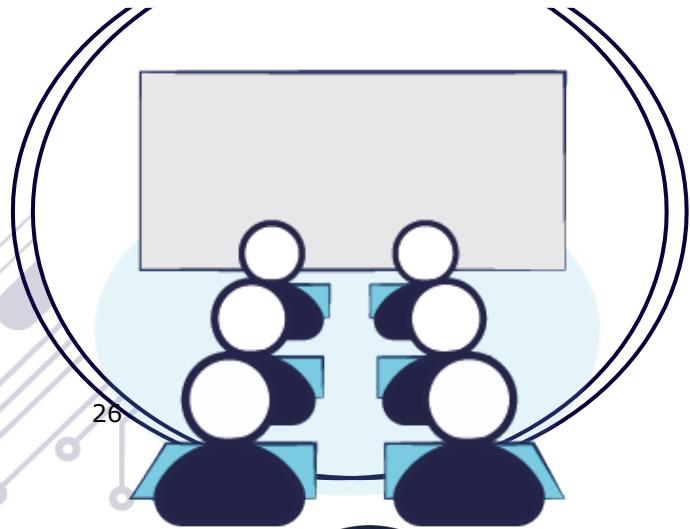
C'est une question technique



C'est une question organisationnelle



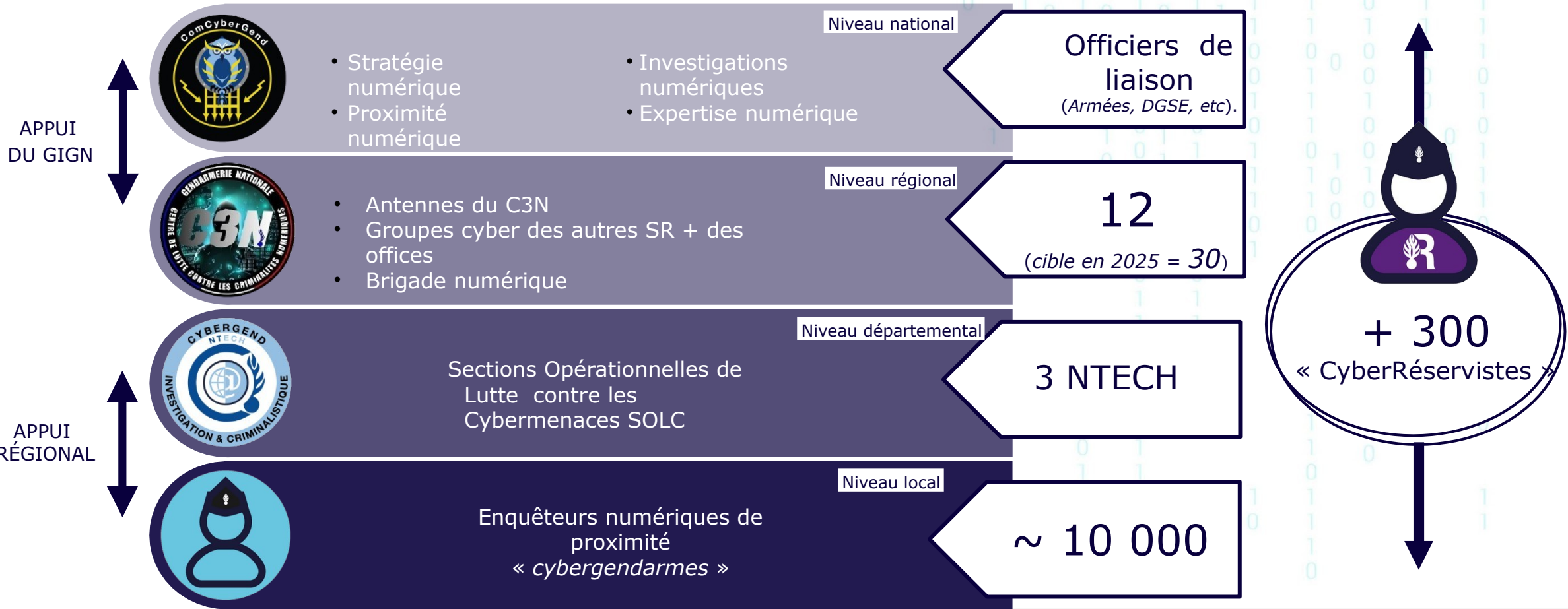
C'est une question de sensibilisation / prévention



26



# PRINCIPE DE SUBSIDIARITÉ ASSOCIÉ À UNE CAPACITÉ DE GESTION DE CRISE COMPLÉMENTAIRE





## UNE ANNÉE 2022 DENSE

### PREVENTION/FORMATION



**368**  
interactions/j



**441 000**  
Personnes / entités  
sensibilisées



**CNF**  
Lille

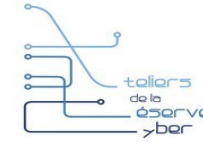
### STRATÉGIE PLURIELLE



Plan d'action  
cyber 2022-2025  
5 axes – 9 actions



Coopération  
internationale  
partenariats  
*Expert reconnu à l'international  
Poursuite des partenariats*



Réserve Cyber  
& + de 300 réservistes 4  
temps forts / an  
Renforts opérationnels  
& stratégiques



Création de la  
filière cyber  
10 000 cyber enquêteurs  
Montée en puissance  
des effectifs & compétences

### INVESTIGATION



**101 000**  
procédures  
Judiciaires traitées

**PERCEV@L**

**305 000**  
signalements de fraudes  
bancaires pour 161 M€  
de préjudices

### APPUI TECHNIQUES

**150**

outils numériques  
développés en  
propre

**8-9**

experts projetés  
en appui-terrain  
chaque semaine



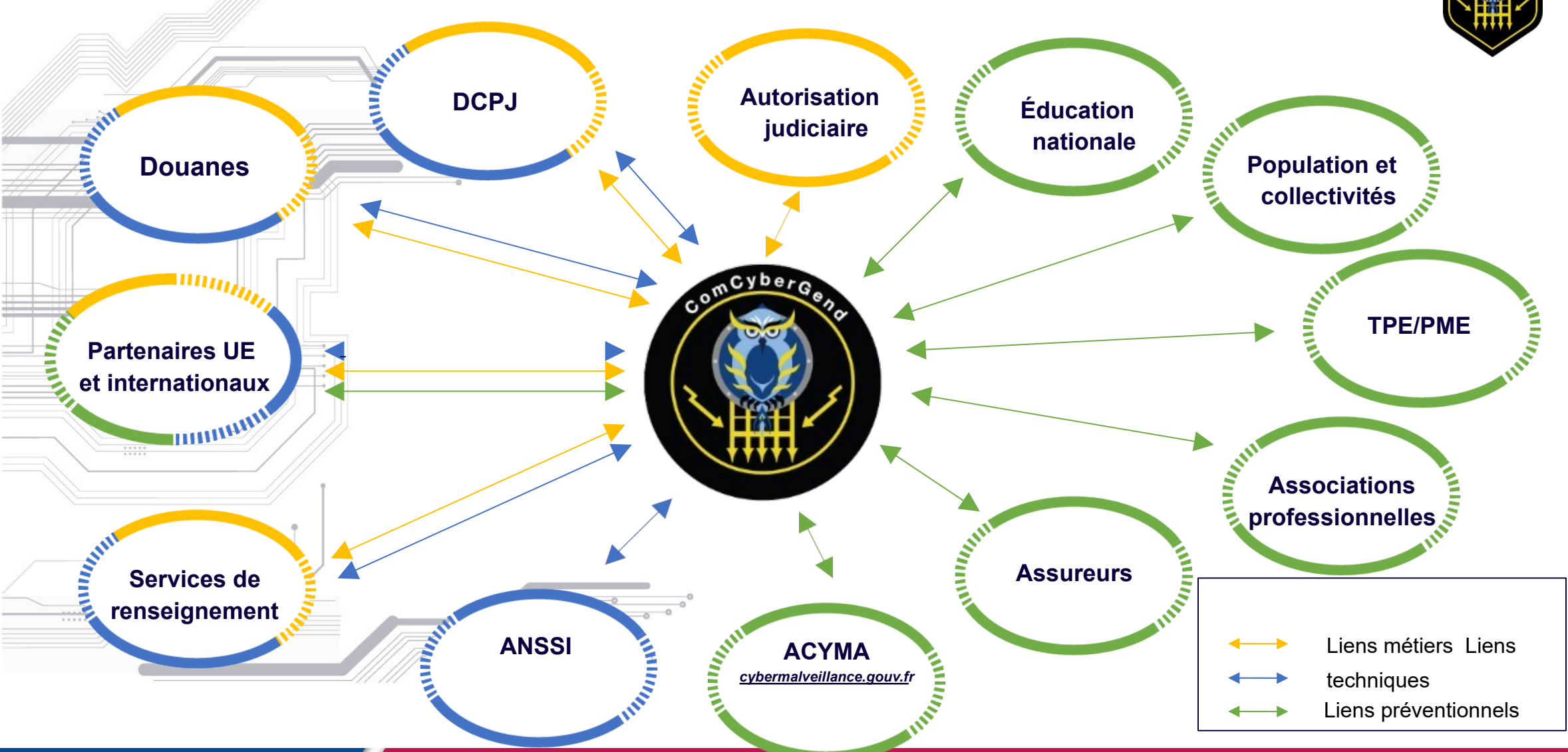
**7 000**  
sollicitations du  
GUTI  
(y compris  
par les partenaires PN,  
douanes,...)



**215**  
réquisitions de haut  
niveau de nos experts  
(cadre judiciaire)



# UN ECOSYSTÈME DE COOPÉRATION DENSE





# Les Advanced Persistent Threats (APT) \*

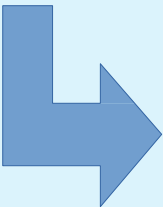
## C'est quoi...

C'est campagne d'attaque complexe

C'est de la criminalité organisée

C'est une cible particulière

C'est un haut niveau technique



### ...Y remédier :

- Surveillance du réseau
- Applications et gestion des droits
- Contrôle d'accès
- Mise à jour et PSI

## ...comment

C'est une compromission des ressources WEB, Réseau ou humaines

C'est l'installation d'une porte dérobée ou d'un logiciel malveillant

C'est une expansion vers les droits administrateurs

C'est une extraction des données sensibles

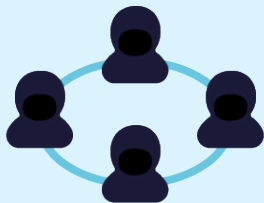


\* Menaces avancées persévérantes

2024 DEVRA ALLIER VISION GLOBALE ET CHOIX STRATÉGIQUES



Des prédictions inquiétantes...



Industrialisation des attaques (RaaS, etc.) avec méthodes d'extorsion dures



Le cyber = arme géopolitique utilisé par des cybermercenaires ?

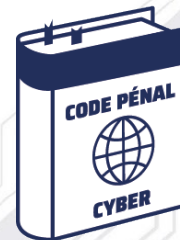


Des surfaces d'attaque supérieures (5G, travail à IoT, Metavers, etc) avec des fuites de données à prévoir



Haine en ligne, deep fake, etc. La manipulation des populations => déstabilisation sociale

...qui nécessitent une approche volontariste et partenariale



Coordonner et adapter la réponse en fonction des infractions



Augmenter les compétences judiciaires et techniques sur le haut du spectre



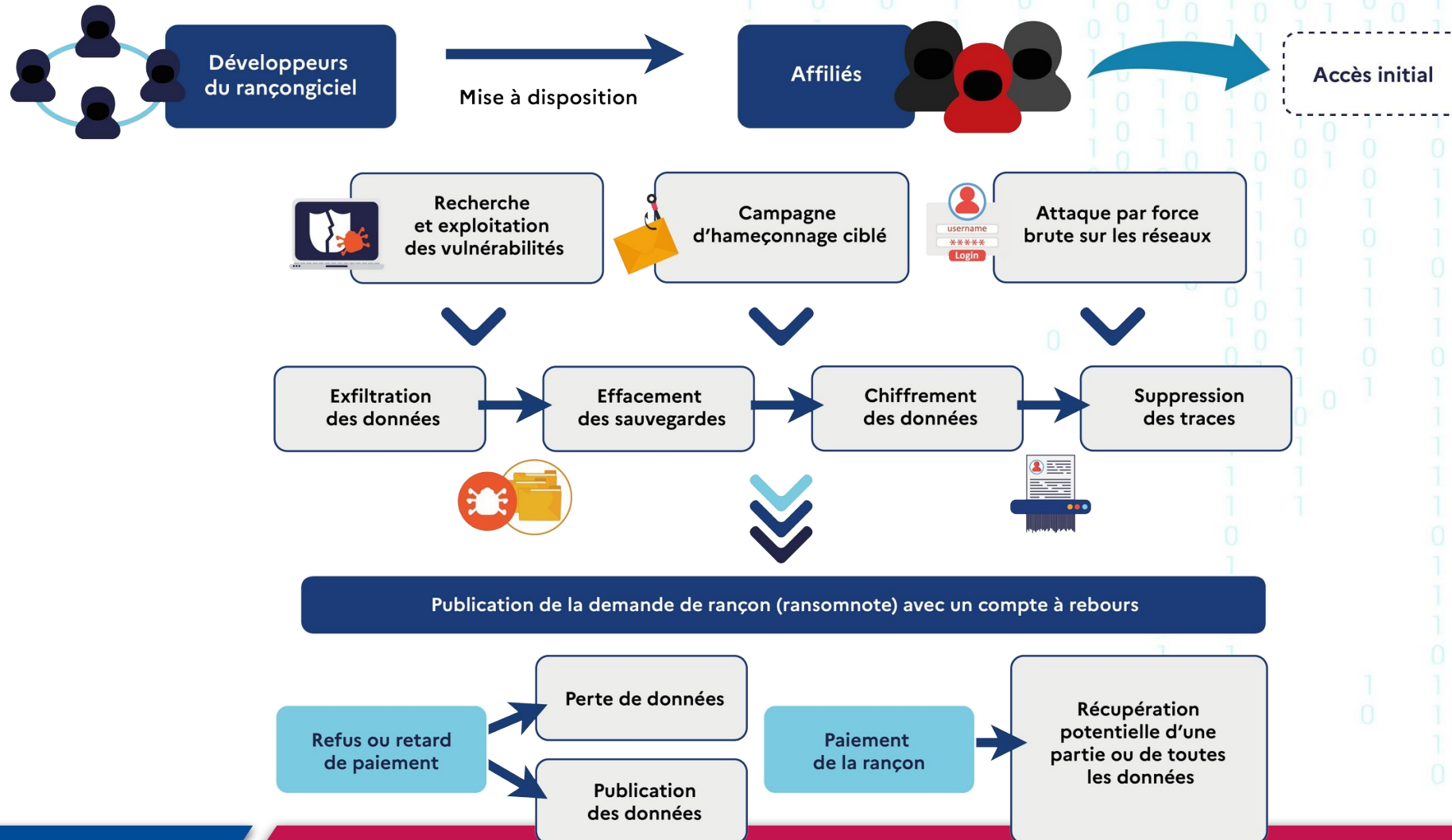
Innover en matière de sensibilisation pour toucher le plus grand nombre



Renforcer les partenariats en France et à l'international, notamment au sein de l'UE



# MODÉLISATION D'UNE CYBERATTAQUE PAR RANÇONGICIEL





## USAGES CRIMINELS



Les phénomènes criminels en lien avec les fuites de données peuvent être regroupés en cinq principales catégories



Atteintes aux personnes :  
Atteinte à la vie privée, harcèlement,  
chantage, sextorsion, etc.



Escroqueries :  
Récupération de RIB, de numéros de carte  
bancaire, de données de santé, etc.



Atteintes aux systèmes de traitement  
automatisé de données (ASTAD) : Toute  
connexion illicite à un compte client en  
ligne constitue une ASTAD.



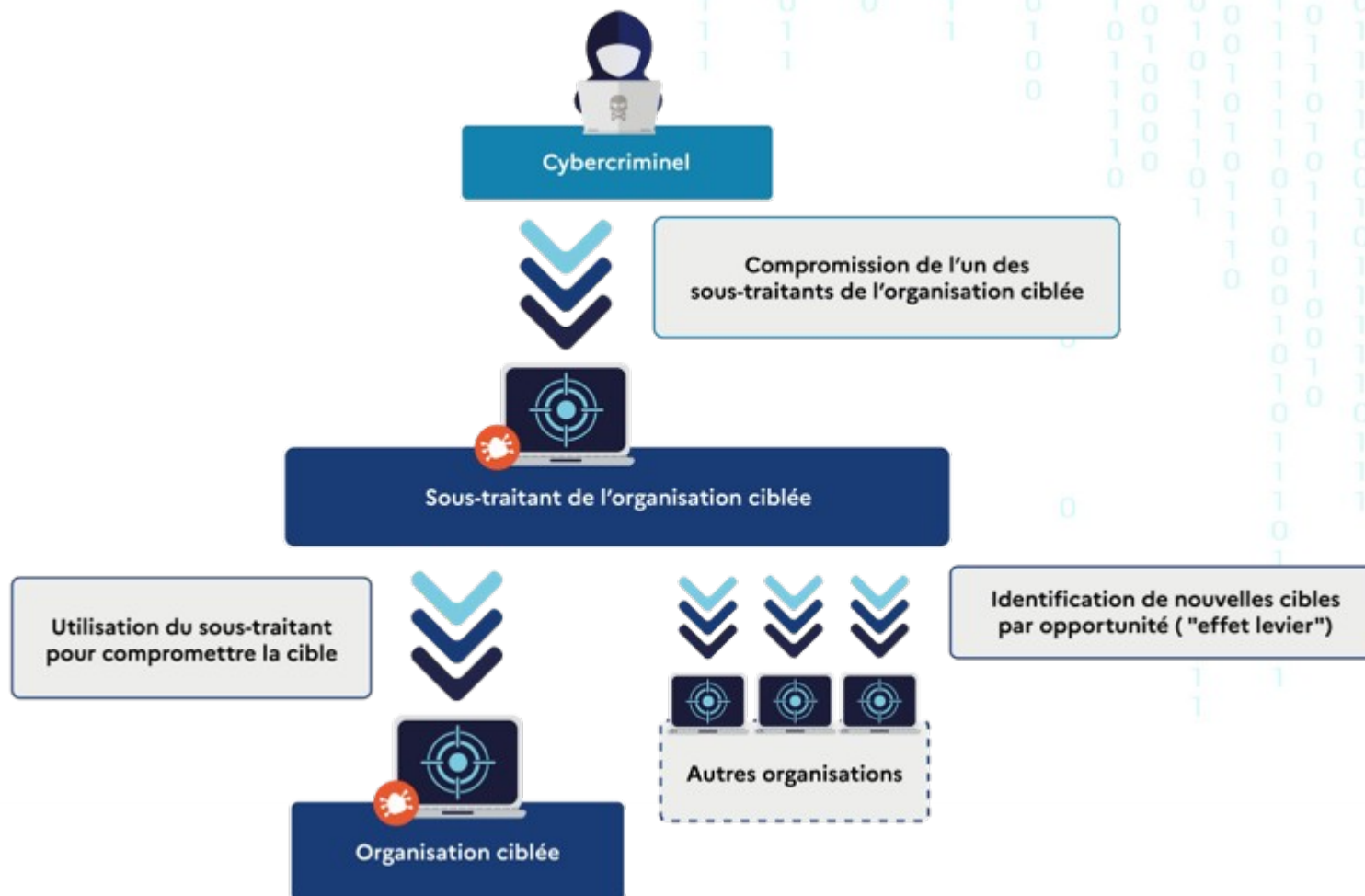
Intelligence économique :  
Des nombreuses informations concernant des  
entreprises sont vendues ou mises à  
disposition par les cybercriminels  
(commerciales, RH, brevets, etc.).



Atteintes à la sécurité nationale :  
Les diffusions de données piratées auprès d'administrations publiques  
tendent à se développer et peuvent porter de graves  
atteintes à la sécurité nationale, notamment en matière de  
terrorisme ou d'ingérence étrangère.



## MODÉLISATION D'UNE ATTAQUE PAR INFILTRATION D'UN SOUS-TRAITANT



# POUR CONCLURE



Collaboration obligatoire entre les cyberacteurs



Le CCG sur l'ensemble du spectre...  
(prévention, domaine technique, dark web, cryptoactifs, pédocriminalité, etc.)



... et sur l'ensemble du territoire français



Le cyber = enjeu majeur actuel (menaces) et futur (grands événements à venir)



MINISTÈRE  
DE L'INTÉRIEUR  
ET DES OUTRE-MER

*Liberté  
Égalité  
Fraternité*

Gendarmerie nationale



MERCI POUR VOTRE ATTENTION



**Adjudante Elena VALLEJO**  
**Sébastien DUPENT**  
**Jean-Charles RENAUDIN**  
**Audrey GERBAUD**  
**Pierre VEUTIN**

**Table ronde 1 :**  
**Connaissance de l'invisible**



# Au cœur d'une cyberattaque : les étapes

Par l'adjudante Elena VALLEJO et Sébastien DUPENT  
Avec la participation des étudiants en BTS SIO option SLAM du lycée René CASSIN



# Le centre d'assistance de proximité Grand Est Cybersécurité

Par Jean-Charles RENAUDIN



# Grand Est Cybersécurité

CENTRE D'ASSISTANCE DE PROXIMITÉ

Piloté par



Opéré par



Soutenu par





## CSIRT (Computer Security Incident Response Team)

**Centre de Réponse d'Urgence  
aux incidents de Cybersécurité  
GRAND EST CYBERSECURITE**

**Le projet s'inscrit dans un dispositif de CSIRT régionaux homogènes et interopérables.**

Le CSIRT permet de :

- **renforcer le niveau de cyber-résilience** du territoire
- **favoriser la mise en relation entre les prestataires et les utilisateurs** de cybersécurité
- agir comme un **outil d'appui au plan de relance et de transformation régional.**

# 0970 512 525

(appel non surtaxé)

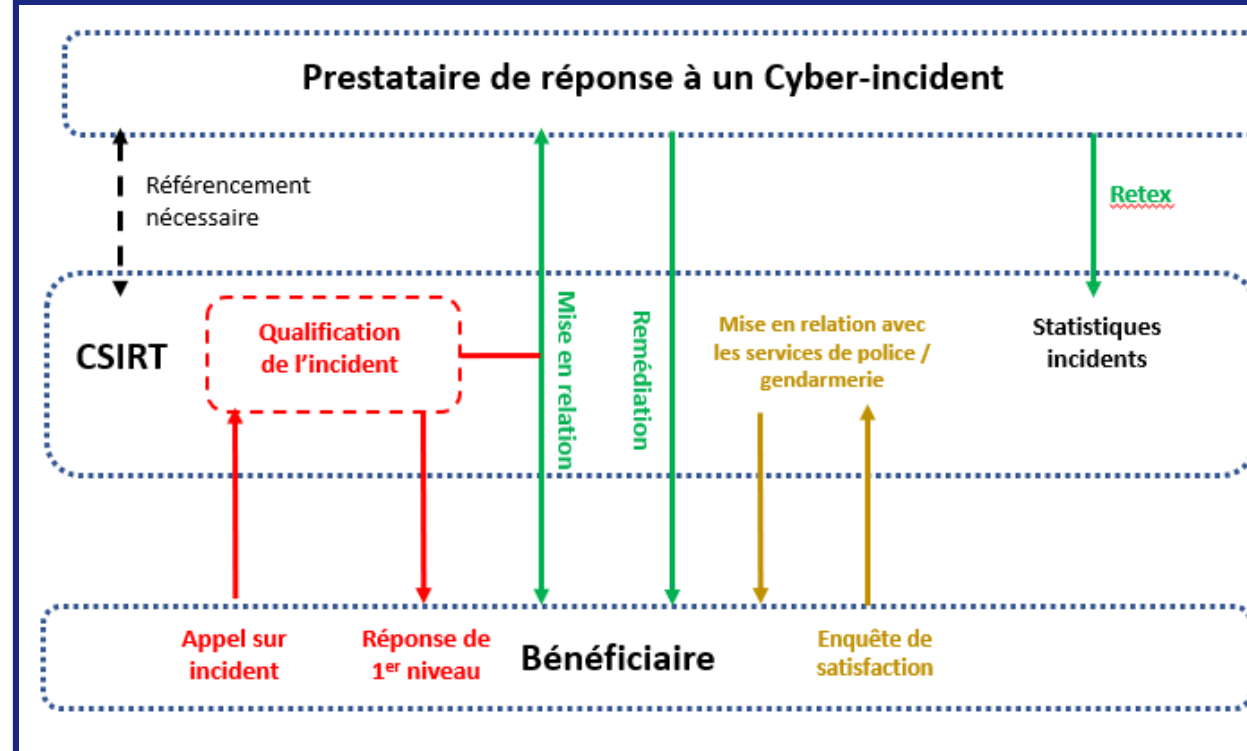
[cybersecurite.grandest.fr](https://cybersecurite.grandest.fr)



dépôt sécurisé

**Grand Est Cybersécurité** délivre du lundi au vendredi (hors jours fériés), **un service de réponse adapté aux besoins** qui comporte des **missions d'intérêt général gratuites** :

- Prise en compte de 1<sup>er</sup> niveau de l'incident avec **pré-diagnostic et qualification**
- **Mise en relation** avec un prestataire qualifié et référencé de réponse à un cyber-incident
- **Suivi / coordination du traitement de l'incident** jusqu'à sa clôture
- **Mise en relation avec les services de police / gendarmerie**
- **Consolidation des statistiques d'incidentologie** à l'échelle régionale
- **Relais et transfert des informations pertinentes** vers le CERT FR, Cybermalveillance, et les autres CERT & CSIRT.



## Bénéficiaires

- **PME / ETI**
- **Collectivités territoriales**
- **Etablissements publics territoriaux**
- **Associations de taille significative**

Les **particuliers**, les **TPE** et les **petites collectivités** sont soutenus par le **GIP ACYMA** [cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr)

Les **Grandes entreprises**, les **Opérateurs d'Importance Vitale (OIV)** et les **Opérateurs de Services Essentiels (OSE)** sont pris en compte par le **CERT-FR de l'ANSSI**



## Mise en oeuvre



Localisation : **Nancy**

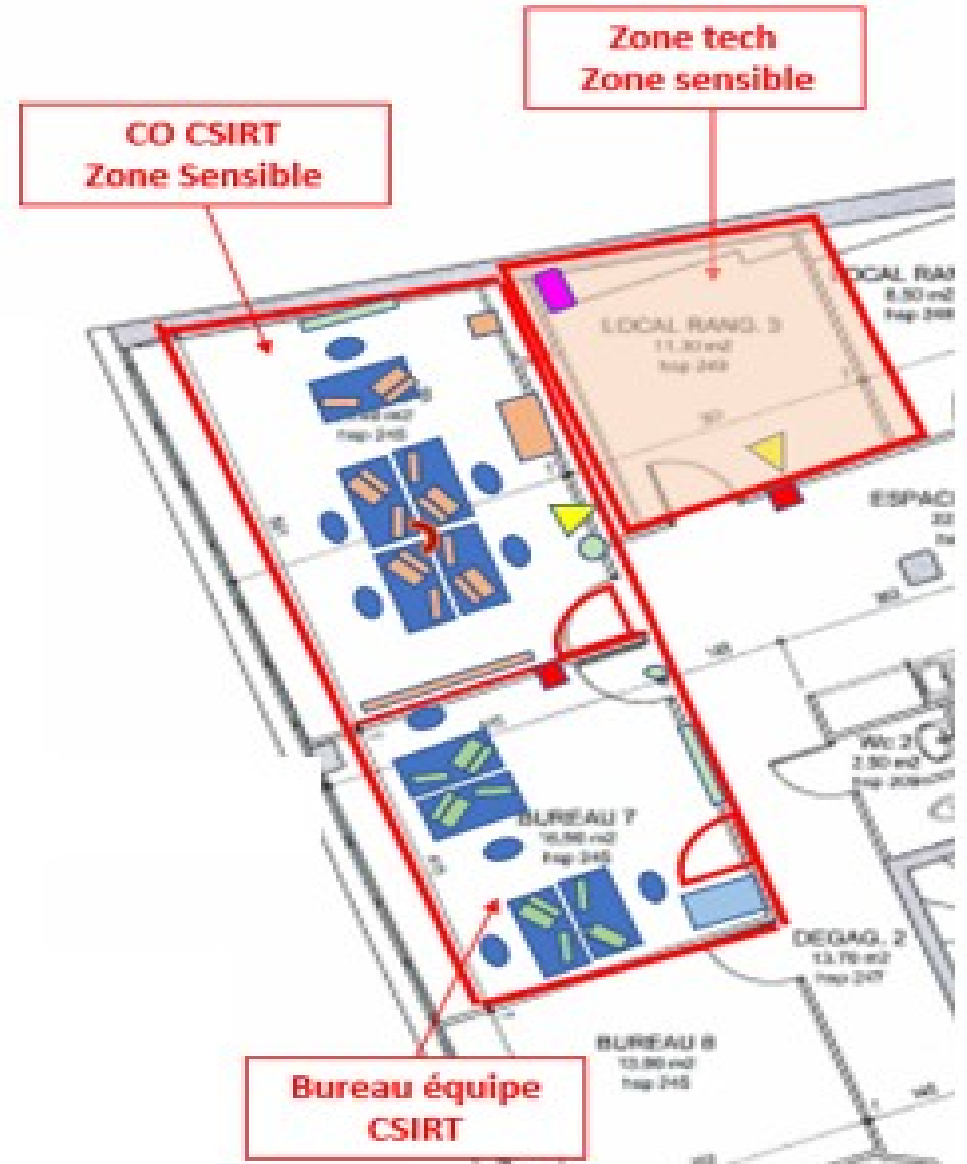
Ouvert depuis le **14 février 2023**

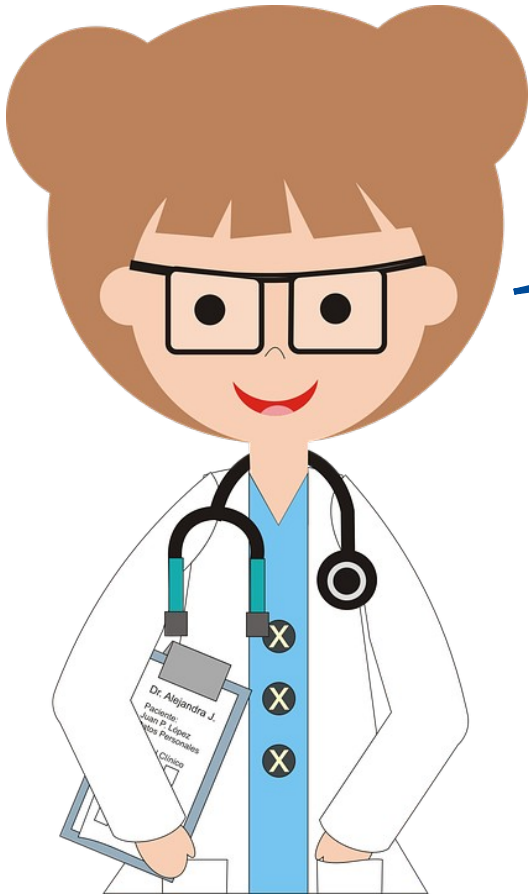
# 0970 512 525

(appel non surtaxé)

09h00 à 12h30 et de 14h00 à 17h30, du lundi  
au vendredi (hors jours fériés)  
> dispositif HNO en cas d'urgence

[cybersecurite.grandest.fr](https://cybersecurite.grandest.fr)





**Vous vous interrogez sur la capacité de votre entreprise à faire face aux cyberattaques ?**

**=> Vous souhaitez réaliser un diagnostic pour évaluer votre niveau de maturité en cybersécurité et définir un plan d'actions.**

Bénéficiez du dispositif régional :

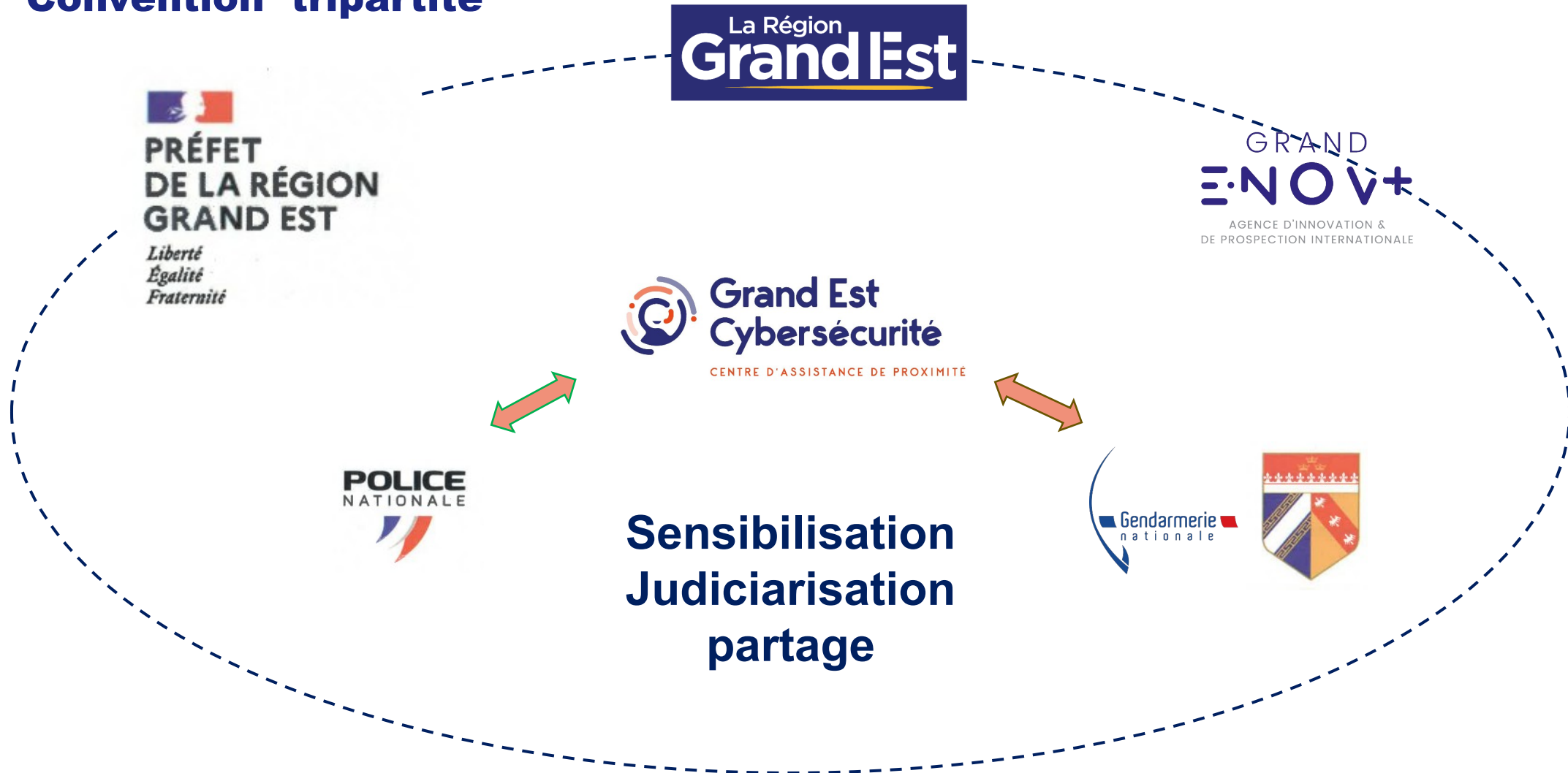
Des **dépenses remboursées jusqu'à 50%** du montant de la **prestation plafonnée à 10 000€ HT** et d'une durée de **10 jours**

**Diagnostic cybersécurité – GrandEst**

**=> Vous souhaitez prévenir les vulnérabilités qui pèsent sur votre infrastructure visible sur Internet :**

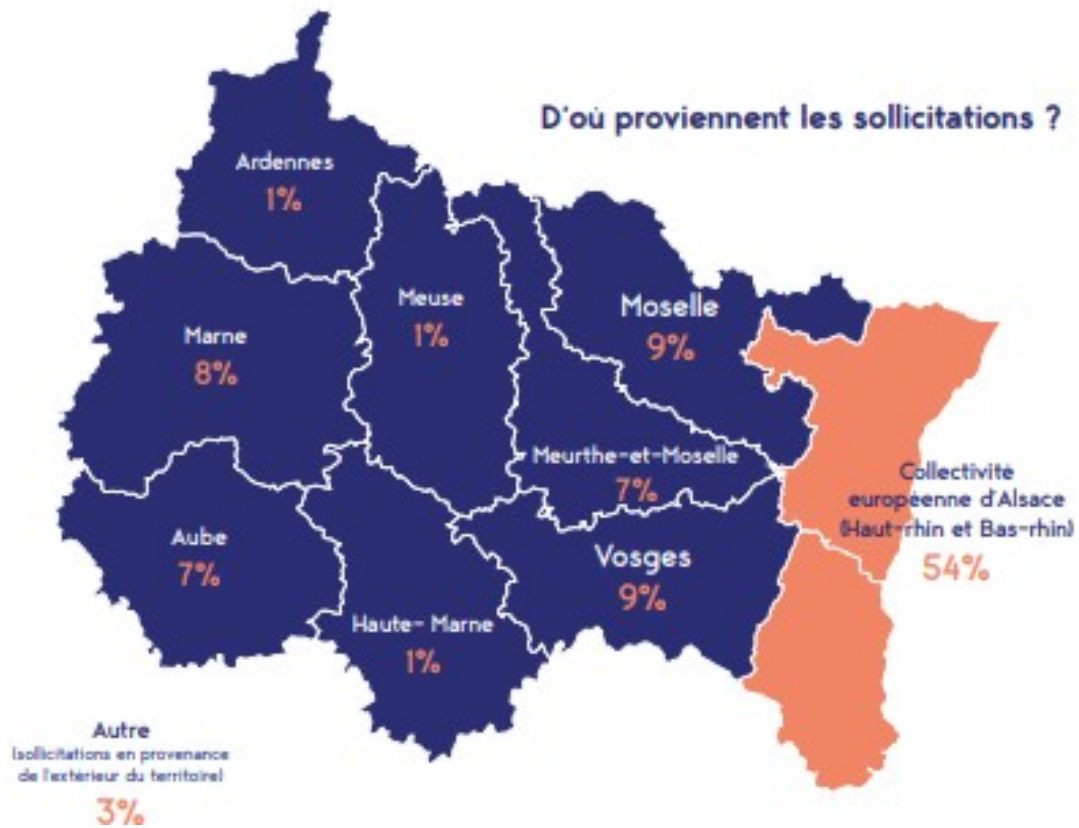
**Scan ANSSI de vos adresses IP Publiques**

## Convention tripartite



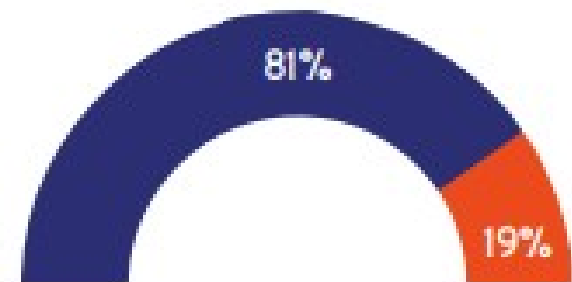
# Synthèse de l'activité Grand Est Cybersécurité

1<sup>er</sup> octobre 2023

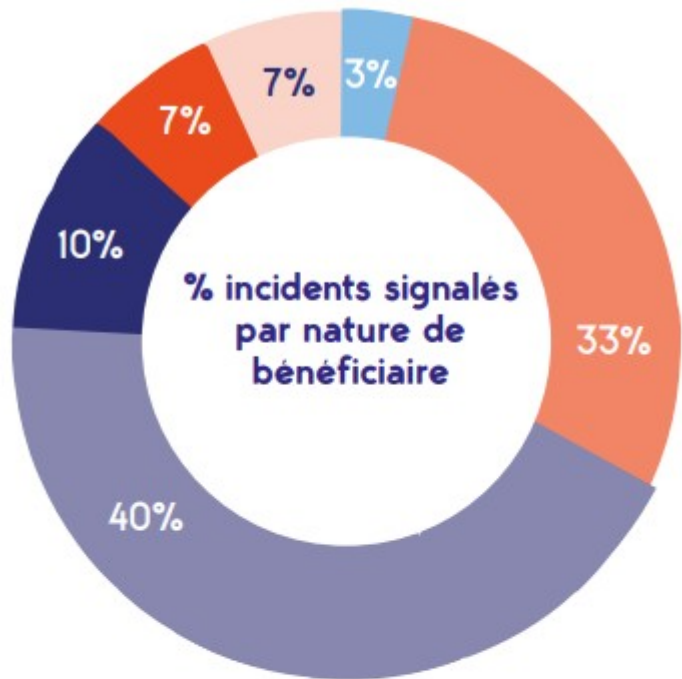


**155** sollicitations reçues

### Nature des sollicitations

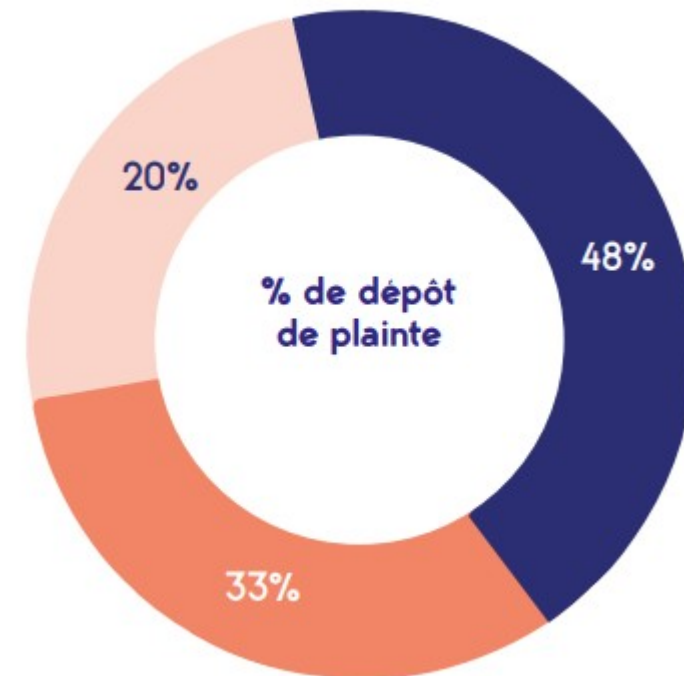
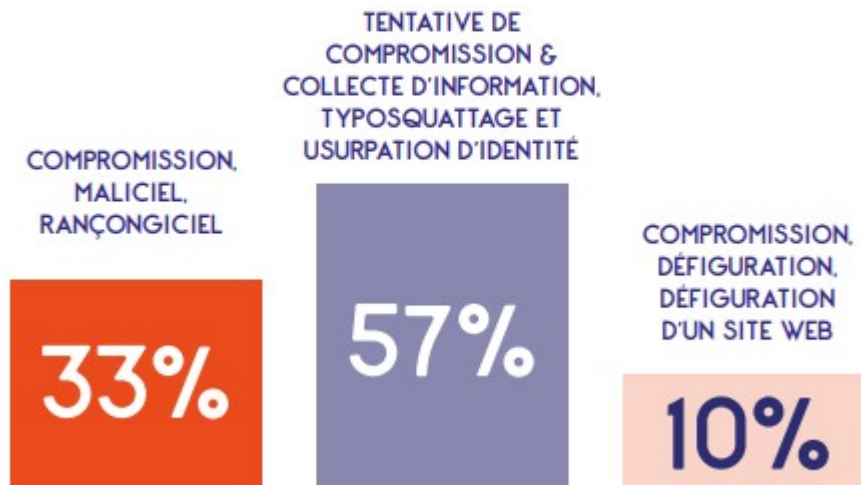


- INCIDENTS
- DEMANDES : AUTRES SOLLICITATIONS (HORS INCIDENTS) EN VUE D'OBTENIR UN RENSEIGNEMENT, OU BÉNÉFICIER DU SERVICE DE SCAM DE L'ANSSI...



- PME
- AUTRES\*
- ETI
- ASSOCIATION NATIONALE AVEC ANCRAGE LOCAL
- COMMUNAUTÉ URBAINE D'AGGLOMÉRATION DE COMMUNES
- AGENCE

**% d'incidents par taxonomie (référentiel ANSSI)**



- NON
- OUI
- PAS CONNAISSANCE\*

\*LE BÉNÉFICIAIRE N'A PAS COMMUNIQUÉ SA POSTURE VIS-À-VIS DU DÉPÔT DE PLAINTÉ.

\*APPELS EN PROVENANCE DE PARTICULIERS, ET DE TPE DU TERRITOIRE, AUXQUELS S'AJOUTENT DES APPELS QUI PROVIENNENT DE L'EXTÉRIEUR DU TERRITOIRE.





# Grand Est Cybersécurité

CENTRE D'ASSISTANCE DE PROXIMITÉ

0970 512 525



[cybersecurite.grandest.fr](https://cybersecurite.grandest.fr)

Piloté par

La Région  
**Grand Est**

Opéré par

GRAND  
**ENOV+**  
AGENCE D'INNOVATION &  
DE PROSPECTION INTERNATIONALE

Soutenu  
par

  
**RÉPUBLIQUE  
FRANÇAISE**  
*Liberté  
Égalité  
Fraternité*





# Dépôt de plainte, constitution du dossier

Par la substitute Audrey GERBAUD

# Organisation judiciaire de la lutte contre la cybercriminalité

Un service spécialisé à compétence nationale : la section J3 du parquet de Paris

- 5 magistrats, 2 greffiers, 2 assistants spécialisés et 1 juriste assistante
- Compétent pour les ASTAD
- 3 niveaux de compétence : parisien / CCN / JUNALCO

Un maillage territorial étoffé : le réseau des cyber-référents

- Un référent par parquet
- Compétent pour l'ensemble des infractions commises sur le ressort de son tribunal
- Echanges directs avec J3

# Rôle du parquet

- Diriger l'enquête
- Assurer la coopération judiciaire internationale
- Apprécier les suites à donner
- A l'audience : représenter le ministère public
- Après la condamnation : s'assurer de l'exécution de la peine prononcée

## Information du parquet

- Compte-rendu d'un service d'enquête
- Remontée d'un autre parquet
- Courrier de la victime
- Autre : presse, partenaires, article 40 CPP...

# Pourquoi déposer plainte ?

- Une obligation imposée par la LOPMI depuis le 24 avril 2023 - L12-10-1 code des assurances. Délai : 72h.

Mais **surtout**, au plan pénal :

- Comprendre le mode opératoire des cyberattaquants
- Identifier les auteurs
- Interpeller les cybercriminels

Avec un **enjeu de taille** :

- La préservation de la « scène de crime numérique »

# Les preuves numériques : quel intérêt ?

- Identifier les caractéristiques de l'attaque dans le réseau :
  - Premier poste compromis
  - Origine de la compromission
  - Ressources / logiciels utilisés par les attaquants
  - Technique de latéralisation
- Rapprochement avec des modes opératoires déjà connus, voire attribués
- Identification des serveurs d'attaque

# Les preuves numériques : quelles sont-elles ?

En-têtes de mail complets

Notes de rançon / échanges  
avec les cyberattaquants

Fichier infecté

Logs de connexion

Identification voire  
extraction des outils  
d'attaque

Fichiers chiffrés : extension

Rsw : souche récupérée ?

# Les preuves numériques

## Difficultés

- Importante volatilité
- Articulation avec les mesures de remédiation
- Difficulté d'accès :
  - chiffrement
  - anonymisation
  - extranéité

## Solutions

- Gel des données
- Coopération internationale
- Enquête sous pseudonyme
- Tracing
  - Pertinence et efficacité soumises à la rapidité



# Comment déposer plainte ?

- **Par qui ?**

- la personne qui en a juridiquement la capacité
- le RSSI ou toute personne pouvant expliquer techniquement l'attaque

- **Comment ?**

- rapidement
- en apportant autant d'éléments techniques que possible : cf formulaire R2iP

- **Auprès de qui ?**

- le commissariat ou la gendarmerie territorialement compétente
- gain de temps : pré-plainte en ligne

- **En complément :**

Cybermalveillance : un organisme public dédié à la prévention et à l'assistance.

# En annexe : formulaire R2IP

1. Saisine [1. OPENING CASE FILE]		3. Infrastructure d'attaque [3. INFRA]	
1.1	Date des faits	3.1	Vecteur d'infection
1.2	Service de plainte (CSP-BTA)	3.2	Date de l'infection
1.3	Parquet local	3.3	Identification du poste primo-infecté
1.4	JUNALCO / Section J3 avisée	3.4	Préservation du poste primo-infecté
1.5	DCPJ avisée	3.5	Logs d'infection (IP + horodatage + fuseau horaire)
2. Victime et premiers intervenants [2. VICTIM & FIRST RESPONDERS]		3.6	Cheval de troie (Emotet, Dridex, Trickbot...)
2.1	Nom de la victime	3.7	Programme de déploiement (Cobalt strike, mimikatz...)
2.2	Adresse	3.8	Préservation des exécutables (.exe)
2.3	N° SIRET	3.9	Outils d'attaque utilisés
2.4	Type victime		Extraction de ces outils
	Secteur économique	3.10	Autres programmes d'attaque utilisés
2.5	Point de contact	3.11	Date du chiffrement des données
2.6	RSSI/DSI Victime	3.12	Destination (IP, URL) des données extraites du SI
2.7	Nom société réponse à incident	4. Vecteur de communication [4. COM]	
2.8	Responsable société réponse à incident	4.1	Contact avec les auteurs
2.9	Famille rançongiciel	4.2	Adresse ou lien de contact
2.10	Souche récupérée	4.3	Négociations débutées
	Si oui, Hash	4.4	Autorisation de négociation par forces de l'ordre
2.11	Extension fichiers chiffrés	5. Vecteur financier [5. FIN]	
2.12	Logs (IP + date et heure + fuseau horaire)	5.1	Paiement de la rançon
2.13	Logs disponibles	5.2	Montant de la rançon
2.14	Note de rançon annexée	5.3	Adresse de paiement
2.15	Impact sur l'activité de la société	5.4	Types de cryptomonnaie (BTC, MONERO, ETH,...)
2.16	Une ou plusieurs machines du réseau sont-elles accessibles à distance ?		
	Comment ?		
2.17	Les serveurs chiffrés avaient-ils accès à Internet en direct ?		
2.18	VM en cours de chiffrement disponible (format .vmk, .vhdx, E01 etc...)		
2.19	Possibilité de mettre en place un SFTP pour la transmission des données		
2.20	Domaine public (web, VPN, Citrix,...)		
2.21	I.P. publique de la société		

# Après la plainte : quelles suites ?

- **Où va la plainte ?**

- CR au parquet
- Infraction commise à Paris : J3
- Infraction commise ailleurs : au cyber-référent, ou à J3 selon la complexité

- **Comment être informé des suites ?**

- Automatiquement en cas de poursuites.
- Par un courrier au parquet, en indiquant : date des faits, raison sociale, date et lieu de la plainte

- **« Je n'ai pas de nouvelle, il ne se passe rien »**

- Principe fondamental de l'enquête : le secret. Article 11 CPP
- Temps long : complexité des investigations

- **« De toutes façons, ils ne sont jamais arrêtés »**

- Interpellations nationales
- Comme internationales !

Quelques exemples ...

# Opérations nationales

## Alternant chez Orange Cyberdéfense le jour, développeur de programmes malveillants la nuit

Sécurité

**Sécurité :** *Un jeune informaticien de l'ouest de la France a été condamné par la justice parisienne. Il avait mis au point un shellcode, un programme d'obscurcissement qui permet de contourner les antivirus.*

## Auteur d'un shellcode redoutable, cet alternant de chez Orange Cyberdéfense file en prison !

📅 28/10/2023 👤 Florian Burnel 👁 166 Views 💬 5 Commentaires 🏷️ Cybersécurité ⌚ 2 min read

Un jeune, encore alternant chez Orange Cyberdéfense, a été condamné par la justice parisienne ! La raison ? Il participait indirectement au développement de logiciels malveillants, grâce à un shellcode devenu populaire, qu'il revendait ensuite sur le dark web !

Ce jeune talent de 23 ans a mal tourné : alors qu'il travaillait chez Orange Cyberdéfense en tant qu'alternant, il a été arrêté dans le cadre d'une affaire de cybercriminalité. Ce mercredi 25 octobre 2023, après **13 mois passés en détention provisoire**, il vient d'être condamné par la 13e chambre correctionnelle du tribunal judiciaire de Paris ! Résultat, il est condamné à **4 ans de prison dont 2 ans avec sursis**, ainsi qu'une **amende de 50 000 euros, dont 40 000 euros avec sursis**. À cela s'ajoute la confiscation de certains scellés et des cryptoactifs détenus sur **2 plateformes**.

# Opérations internationales

Publié le 21 octobre 2023 à 10h43

## Un cybercriminel russe membre du gang Ragnar Locker arrêté en France

## Rançongiciel : un hacker soupçonné d'être l'auteur de 115 attaques en France interpellé au Canada

Ce Russo-Canadien aurait travaillé avec quatre des groupes de pirates les plus importants de ces dernières années – Ragnar Locker, Lockbit, BlackXCat et DarkSide –, faisant plus de 1 800 victimes dans le monde.

PIXELS · RANÇONGICIELS

## Rançongiciels : comment les autorités françaises remontent la trace des cybercriminels

Deux ans après l'explosion du nombre d'attaques par rançongiciel, plusieurs têtes pensantes de ces groupes criminels spécialisés dans l'extorsion ont été identifiées.



This service has been seized as part of a coordinated international law enforcement action against the RagnarLocker group



# Réponse à incident - remédiation - redémarrage

Par Pierre VEUTIN

# Réponse à Incident



Processus en *6 étapes* :

- 1 Préparation
- 2 Identification
- 3 Confinement / Endiguement
- 4 Eradication
- 5 Récupération / Remise
- 6 Capitalisation

# Réponse à incident, Remédiation, Redémarrage

● Les différentes définitions de l'« Incident cyber »

● La « remédiation » vue par les différents acteurs

- Entreprise
- Prestataire (intégrateurs et opérateur « du quotidien »)
- Prestataire spécialisé en Réponse à Incident

● Le « redémarrage » tel qu'il est considéré par le dirigeant VS tel qu'il devrait idéalement être



# Réponse à Incident

## Incident de sécurité – ANSSI



Un incident de sécurité est un événement qui porte atteinte à la **disponibilité (D)**, la **confidentialité (C)** ou l'**intégrité (I)** d'un bien.

## Exemples

- Rançongiciel → **D + I + (C)**
- Utilisation illégale d'un mot de passe (*phishing, leaks*) → **C**
- Vol d'équipements informatiques → **D + C**
- Intrusion dans un fichier ou une application → **C + I**
- Déni de service → **D**
- etc.

# Réponse à Incident

## 1<sup>ÈRE</sup> ÉTAPE : la **détection** ...

*Certaines victimes sont compromises depuis plusieurs mois / années avant que les attaquants ne passent à l'offensive*



### OBJECTIFS

- Gagner du temps
- Réduire l'impact

**Vous avez une responsabilité, vous devez (à l'avance) :**



- ✓ Mettre en place des solutions de **gestion des événements de sécurité**
- ✓ (faire) **Surveiller** les alertes
- ✓ Alerter au plus vite si vous êtes témoin

# Réponse à Incident

## **RETEX** (*mauvaise détection*) :

- Entreprise dans le domaine de l'agroalimentaire
- Sous-traitance complète du volet sécurité de son SI
- Rançongiciel déployé sur l'intégralité du SI bureautique en quelques heures
- Compromission initiale 2 ans avant (obtention des accès)
- Plusieurs traces dans des listes de cibles potentielles sur le dark net et sur des plateformes de scan.



## **SOLUTIONS**

- Surveiller le prestataire
- Faire de la veille

# Réponse à Incident

## 2ÈME ÉTAPE :

basculer en mode **gestion de crise**

*Ça ne s'invente pas, ça se prépare !*

## Vous devez...

- ✓ Disposer d'un **kit de gestion de crise** prêt à l'emploi
  - Qui est **responsable** de quoi / comment le contacter ?
  - En externe, qui doit-on **prévenir** ? (assurance, avocats, services judiciaires, etc.)
- ✓ Avoir **formé vos équipes** en amont
  - Quels sont les **premiers gestes à effectuer** en autonomie en attendant « *les secours* » ?
  - Comment **communique**-t-on en interne / en externe ?
- ✓ Disposer de **toutes les informations à jour**, format numérique ou papier (coffre)



## OBJECTIFS

- Préservez les traces au maximum
- Permettre une bonne analyse de la situation

# Réponse à incident

## **RETEX** (*mauvaise communication*) :

- Entreprise qui subit une attaque par rançongiciel MAZE
- Publication de crise rapide indiquant que :
  - Tout est sous-contrôle
  - Aucune donnée n'a fuité
- 1 semaine plus tard le groupe de cybercriminels publie les données

# Remédiation

## Définition(s) :



*(Éducation)* Mise en œuvre des moyens permettant de résoudre des difficultés d'apprentissage repérées au cours d'une **évaluation**.



*(Gouvernance et audit)* **Établissement d'un plan d'action**, avec des objectifs temps et résultat, accompagné de la mise sur pied d'un **groupe de personnes aptes** à le mettre en œuvre, aux fins de remédier à des **situations insatisfaisantes dans l'organisation** ou le **respect des normes** dans le domaine de la gestion des entreprises ou structures administratives.

*(Wikipédia)*

# Remédiation

## Différentes manières de procéder :

Avec votre *prestataire habituel*



- Il connaît le SI et vos métiers
- Il dispose peut être de sauvegardes !?
- Il a déjà fait le déploiement une fois, pourquoi pas 2



- Il ne connaît pas les bons gestes et risque d'effacer les traces
- Il va probablement se contenter de remonter les sauvegardes
- Son objectif (à peine dissimulé) est de revendre la même prestation (il est peut être responsable en partie de l'incident)

# Remédiation

## Différentes manières de procéder :

Avec votre **prestataire spécialisé**



Il sait comment agir : préservation des traces, confinement des actifs compromis, ...

Il peut vous aider à organiser la cellule de crise et à gérer votre communication

Il vous accompagne sur une prestation de gestion de crise et passe le relai sur ce qu'il ne sait pas faire (intégrateur, développement, etc.)



Il n'est pas là pour vous vendre du matériel mais pour vous aider

Il ne connaît pas votre SI et vos services métiers

Il ne connaît pas forcément toutes les technologies en place



### COMBINAISON IDÉALE

Prestataire *spécialisé* pilote le prestataire *habituel*



# Remédiation

## RETEX (*pas de PCA*) :

- 1 entreprise dans le domaine de la formation
- Administrateur a laissé un accès distant pour la gestion
- Faute de budget mauvaise sécurisation de l'accès
- Aucun document sur l'infrastructure à jour
  - ✗ Perte de temps dans l'intervention de 1 journée



### SOLUTIONS

- Mise en place d'un PCA
- Documentation critique à jour hors ligne

# Redémarrage

## Vite ET Bien



- Où sont vos données (traces / sauvegardes) ?
- Comment y **accède**-t-on ?
- Quelle est la **bande passante** pour les rapatrier ?

## Problème du prestataire « habituel »



- Remonter une **sauvegarde empoisonnée** n'est pas la solution
- Identifier si la sauvegarde est saine nécessite une compréhension de ce qui se passe donc d'avoir fait une **investigation**

# Redémarrage

## RETEX (*pas de PRA*) :

- Même entreprise que RETEX PCA
- Aucune sauvegarde récupérable (règle des 3-2-1 non-respectée)
- Perte de 20 années de travail pour certains employés



### SOLUTIONS

- Documentation critique hors-ligne
- Sauvegardes
- Budget alloué à la SSI

# Conclusion

- **Vous êtes les ~~maillons~~ forgerons de la chaîne de sécurité**
- **Vous avez la responsabilité de :**
  - ✓ Identifier les risques & Définir des politiques de sécurité (décideurs)
  - ✓ Appliquer les politiques de sécurité (administrateurs)
  - ✓ Respecter les politiques de sécurité (utilisateurs)
- **Un prestataire ça *se supervise* quitte à faire appel à un **RSSI à temps partagé pour vous aider** dans la réalisation de cette tâche**





# Nos observateurs spéciaux

# Pause





**Sébastien DUPENT**  
**Sélim-Alexandre ARRAD**  
**Marion PIERRE**  
**Denis MATHIS**

**Table ronde 2 :**  
**Mobilisation et actions**





# Evaluation des risques cyber par une méthode pratique

Par Sébastien DUPENT  
Lieutenant (RC) Gendarmerie Nationale

# Introduction

**Les PME et PMI sont des entités vulnérables.**

PME et PMI (P) sont vulnérables (V) en raison de leur taille restreinte (T) et de leurs ressources limitées (R).

$$\forall P : (T(P) \wedge R(P)) \rightarrow V(P)$$

**Les cyberattaques engendrent des conséquences néfastes.**

Les cyberattaques (C) entraînent des conséquences néfastes (N), notamment des pertes financières (PF), la perte de données sensibles (D), la réputation endommagée (RE), et même la fermeture d'entreprise (FE).

$$C(C) \rightarrow N(C) \equiv (PF(C) \wedge D(C) \wedge RE(C) \wedge FE(C))$$

# L'Analyse de Risque : Une Approche Systématique pour la Cybersécurité



**L'analyse de risque =>  
pilier incontournable pour garantir  
la sécurité des entreprises**

**processus qui permet de d'identifier  
les vulnérabilités des infrastructures informatiques  
et d'anticiper les conséquences de ces menaces.**

**Permet de prioriser les actions de sécurité  
en fonction des risques les plus critiques.**

**permet de gérer les ressources de manière plus efficace,  
en ciblant précisément les failles de sécurité  
qui représentent les risques les plus graves**

# Le Parallèle avec les Risques- INRS

- Il est intéressant de noter que cette approche systématique et logique pour gérer les risques en cybersécurité partage des similitudes avec les principes de gestion des risques professionnels promus par l'INRS.
- Les deux domaines visent à prévenir des conséquences néfastes, qu'elles soient liées à la sécurité des employés ou à la sécurité des données. La démarche consistant à identifier, évaluer et atténuer les risques, ainsi que la priorisation des actions pour une gestion efficace des ressources, s'applique de manière transversale.



# Les différentes normes et méthodes



## Points communs

L'approche de la gestion des risques de sécurité de l'information

## Différence

Leurs méthodes et leur portée

## Le choix

le framework qui convient le mieux au contexte de l'organisation et à ses besoins en matière de sécurité de l'information



## Les différentes étapes de l'analyse des risques cyber

1



### Identification des actifs informatiques

La première étape consiste à identifier tous les actifs informatiques de l'entreprise, tels que les systèmes, les logiciels, les données sensibles et les équipements. Il est important de connaître précisément ce qui doit être protégé.

2



### Évaluation des vulnérabilités

Une fois les actifs identifiés, il est essentiel d'évaluer les vulnérabilités potentielles de chaque actif. Cela inclut l'examen des systèmes obsolètes, des configurations incorrectes, des mots de passe faibles, des accès non autorisés et d'autres facteurs de risque.

3



### Estimation de l'impact des menaces .

À cette étape, il convient d'évaluer l'impact financier, opérationnel et réputationnel que chaque vulnérabilité peut avoir sur l'entreprise. Il est important de considérer les conséquences d'une éventuelle exploitation de ces vulnérabilités.

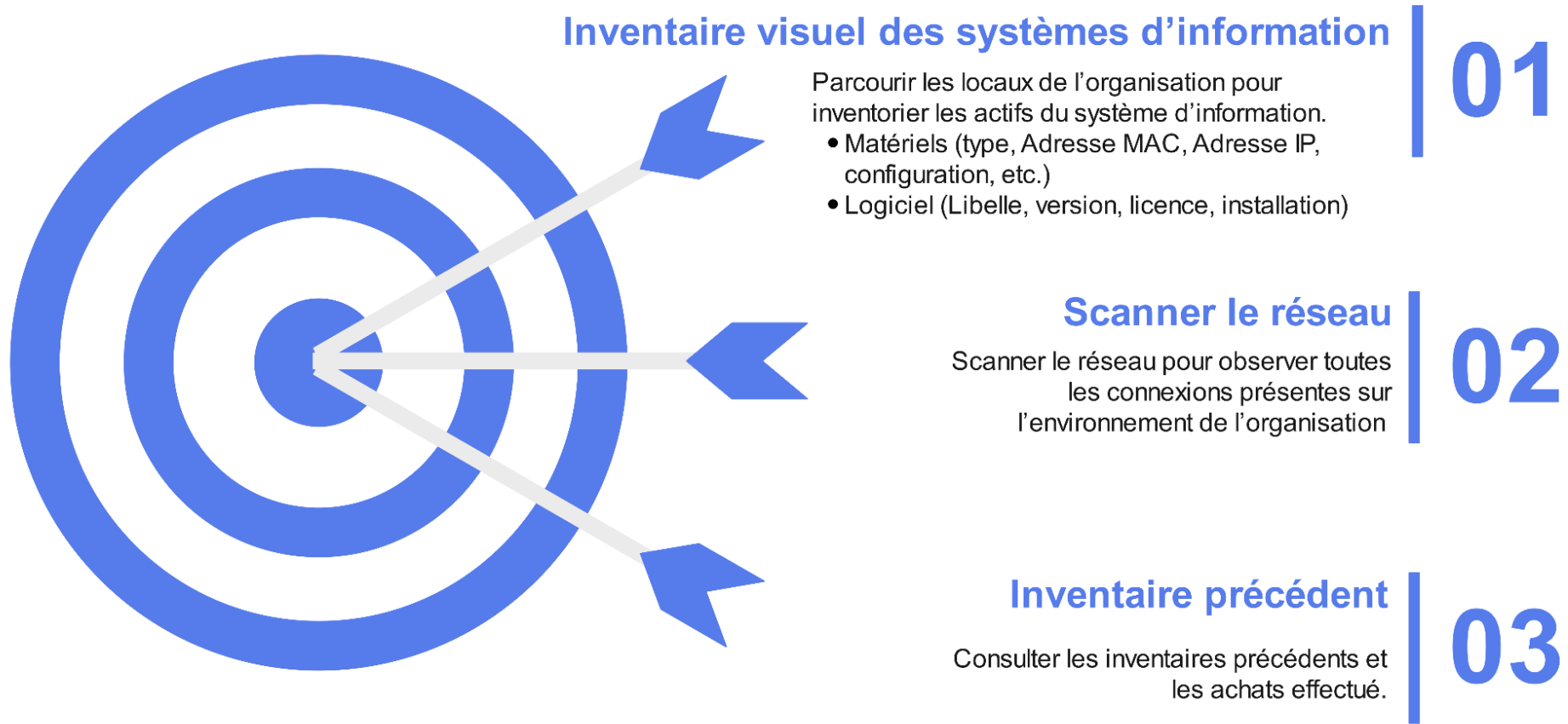
4



### Priorisation des mesures de protection

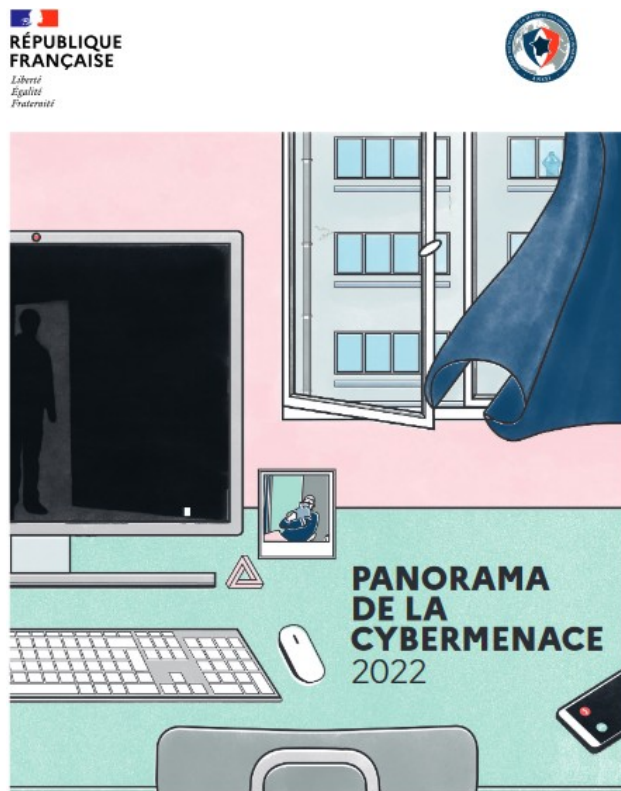
Enfin, il est essentiel de hiérarchiser les mesures de protection en fonction de l'impact potentiel et de la probabilité d'occurrence des menaces. Cela permet de définir une stratégie de cybersécurité efficace et de mettre en place les contrôles appropriés.

# Identification des actifs




# Évaluation des menaces et des vulnérabilités


évaluer les menaces potentielles auxquelles les actifs de l'organisation peuvent être exposés ainsi que les vulnérabilités de ces actifs





Encyclopédie ▾

Encyclopédie de Kaspersky > Base de connaissances > Vulnérabilités et hackers

 **Vulnérabilités des logiciels**  
Beaucoup de menaces d'aujourd'hui exploitent les vulnérabilités de logiciels afin de se propager. En savoir plus sur ce que les vulnérabilités, quelles sont les vulnérabilités les plus courantes sont, et comment les corriger.

 **Comment détecter une attaque de hacker**  
Les pirates peuvent essayer et accéder à votre ordinateur pour avoir accès à vos données ou à utiliser vos ressources informatiques pour l'activité illégale. Cette section fournit des informations sur les signes et symptômes d'une attaque de hacker.

 **Historique du piratage**  
Les systèmes informatiques ont toujours été ciblée par des personnes cherchant soit à améliorer la sécurité ou exploiter les failles. Ce calendrier donne un aperçu des événements majeurs de l'évolution de l'informatique ainsi que l'évolution de piratage.

 **La loi et les hackers**

<https://encyclopedia.kaspersky.fr/knowledge/vulnerabilities-and-hackers/>



<https://www.cyber.gc.ca/sites/default/files/ecmn-2023-24-web2.pdf>



# Estimation des risques

Une fois les menaces identifiées, il faut estimer le risque de chaque menace sur votre organisation en effectuant une appréciation du risque

**MATRICE D'ÉVALUATION DES RISQUES**

PROBABILITÉ QU'UN ÉVÉNEMENT A RISQUE SE PRODUISE

CONSIDÉRER LA GRAVITÉ

	Très peu probable	Peu probable	pourrait arriver	Probable	Très probable
Catastrophique	Modérée	Modérée	Elevée	Critique	Critique
Majeure	Faible	Modérée	Modérée	Elevée	Critique
Modérée	Faible	Modérée	Modérée	Moderatre	Elevée
Mineure	Très faible	Faible	Modérée	Modérée	Modérée
Négligeable	Très faible	Très faible	Faible	Faible	Modérée

© Sébastien DUPENT

# Estimation des risques

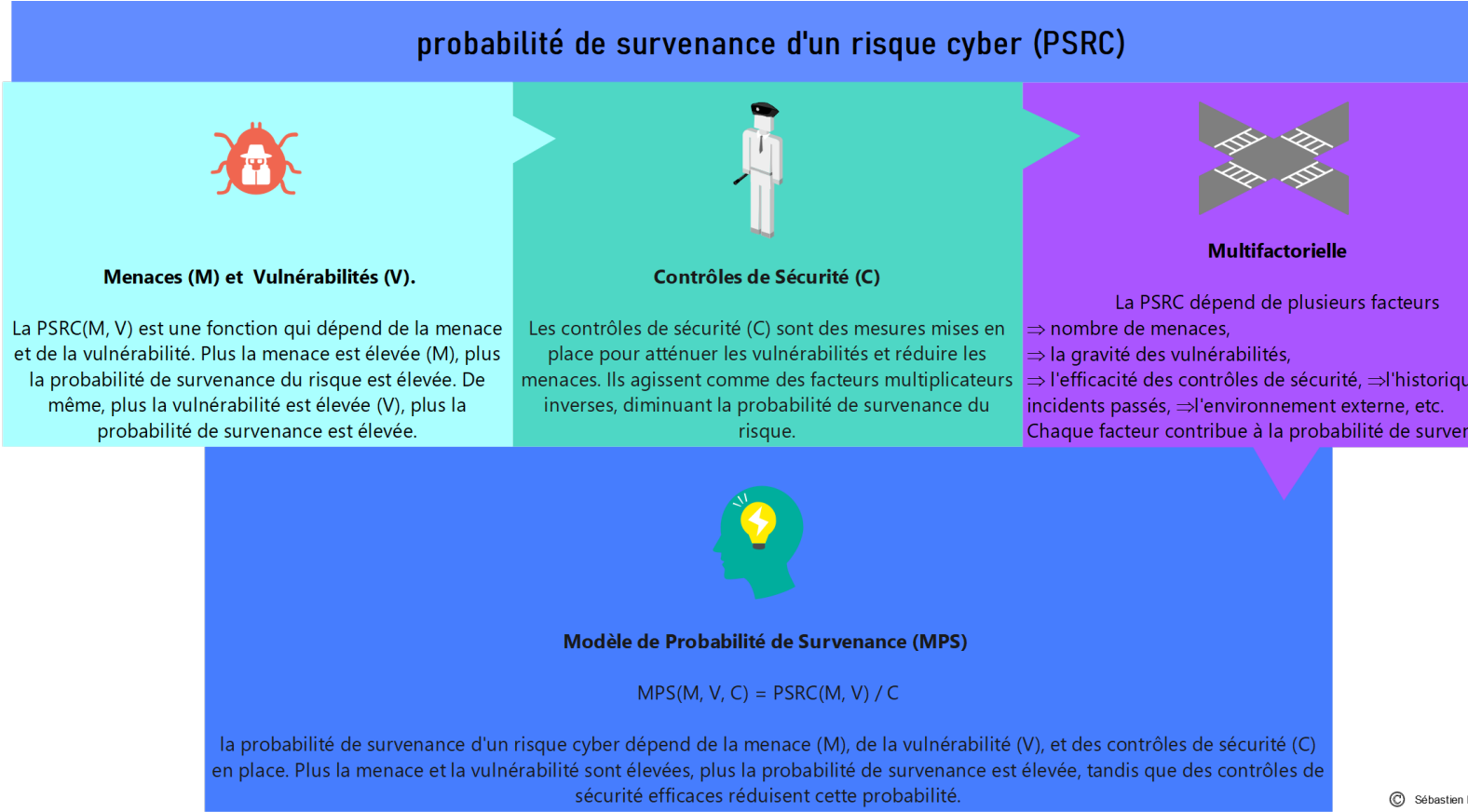
Quelle est la pire conséquence que pourrait entraîner ce risque ?

Quels sont les pires dommages que pourrait entraîner ce risque ?

À quel point sera-t-il difficile de s'en remettre ?

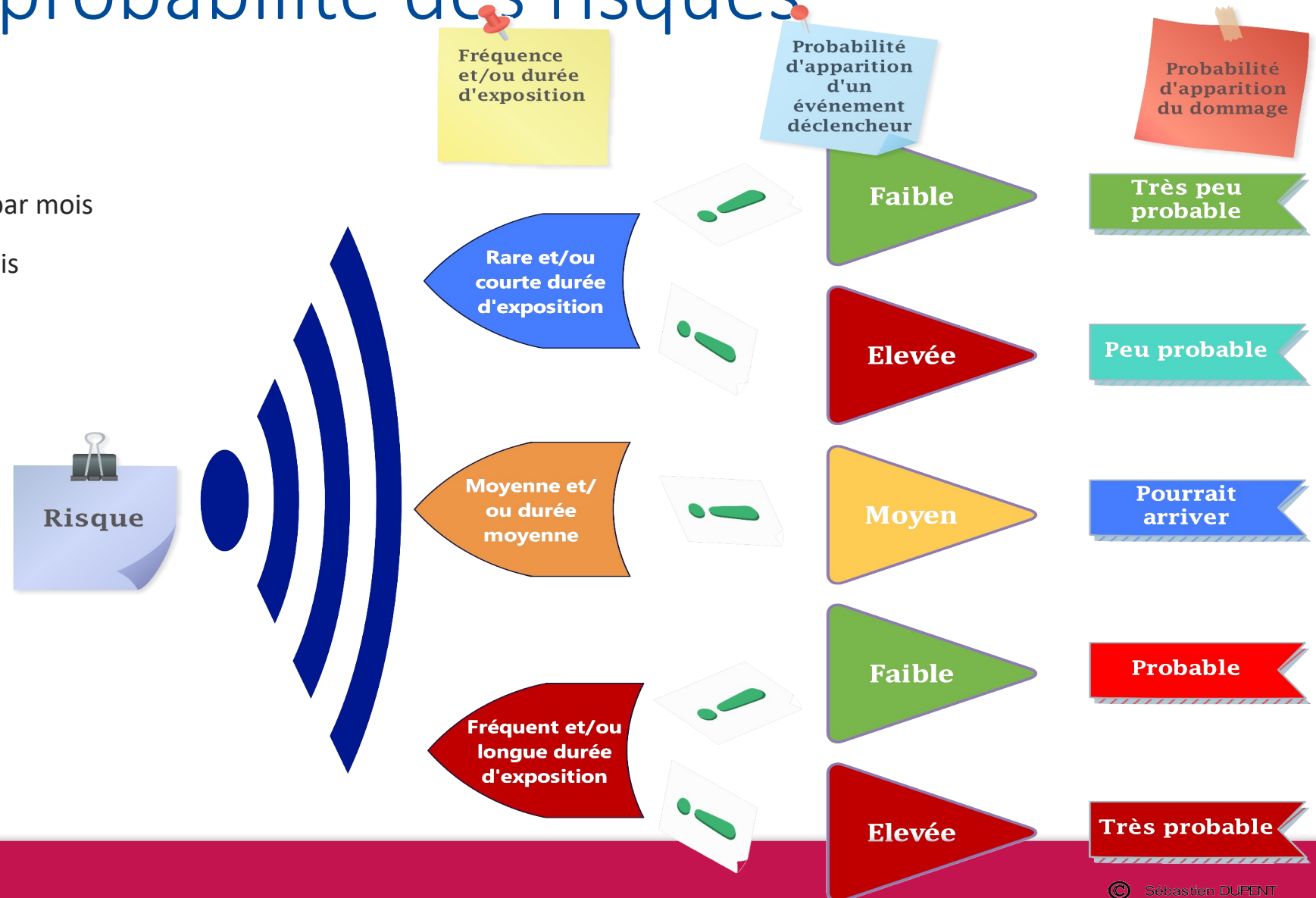
Lequel des cinq niveaux de gravité correspond le mieux à ce risque ?

## la gravité



# Estimez la probabilité des risques

- Exemple de repaire
  - Fréquent = tous les jours
  - Moyenne = au moins une fois par mois
  - Rare = moins d'une fois par mois



# Exemple

kaspersky daily

En résumé, **ne vous fiez pas** aux apparences d'un port USB car il pourrait bien » cacher des choses « . Il s'agit d'un système qui collecte les données des appareils auxquels il est connecté, peu importe les raisons. C'est une source d'énergie bancale, tel un puissant condensateur ou un ordinateur qui installe une porte dérobée sur votre appareil. Une chose que vous ignorez jusqu'à ce que vous le branchez.

phonandroid

Quand on connecte son **smartphone** sur un **port USB**, l'appareil peut à la fois **se recharger**, mais aussi **transférer des données**. Le problème, c'est qu'il n'existe pas de réelle frontière entre les deux technologies : il est donc possible de dérober les données d'un smartphone, alors que l'utilisateur pense simplement recharger son téléphone. Le **juice jacking** fait partie de ces cyberattaques trop souvent ignorées, mais qui peuvent se révéler extrêmement malveillantes pour les victimes. Cette **méthode de piratage** consiste à récupérer les données d'un utilisateur qui pense innocemment recharger son smartphone sur une borne publique, comme on en trouve à foison dans les aéroports, les salons, les restaurants, etc.

Insertion sur un des port USB d'un poste de travail d'un matériel externe à l'entreprise

- Fréquence possible minimum de 30 fois par jours (pour une entreprise de 30 salariés) : Très probable
- Risque : Majeure

**MATRICE D'ÉVALUATION DES RISQUES**

PROBABILITÉ QU'UN ÉVÉNEMENT A RISQUE SE PRODUISE

		PROBABILITÉ QU'UN ÉVÉNEMENT A RISQUE SE PRODUISE				
		Très peu probable	Peu probable	pourrait arriver	Probable	Très probable
CONSIDÉRER LA GRAVITÉ	Catastrophique	Modérée	Modérée	Elevée	Critique	Critique
	Majeure	Faible	Modérée	Modérée	Elevée	Critique
	Modérée	Faible	Modérée	Modérée	Moderatre	Elevée
	Mineure	Très faible	Faible	Modérée	Modérée	Modérée
	Négligeable	Très faible	Très faible	Faible	Faible	Modérée

© Sébastien DUPÉNT

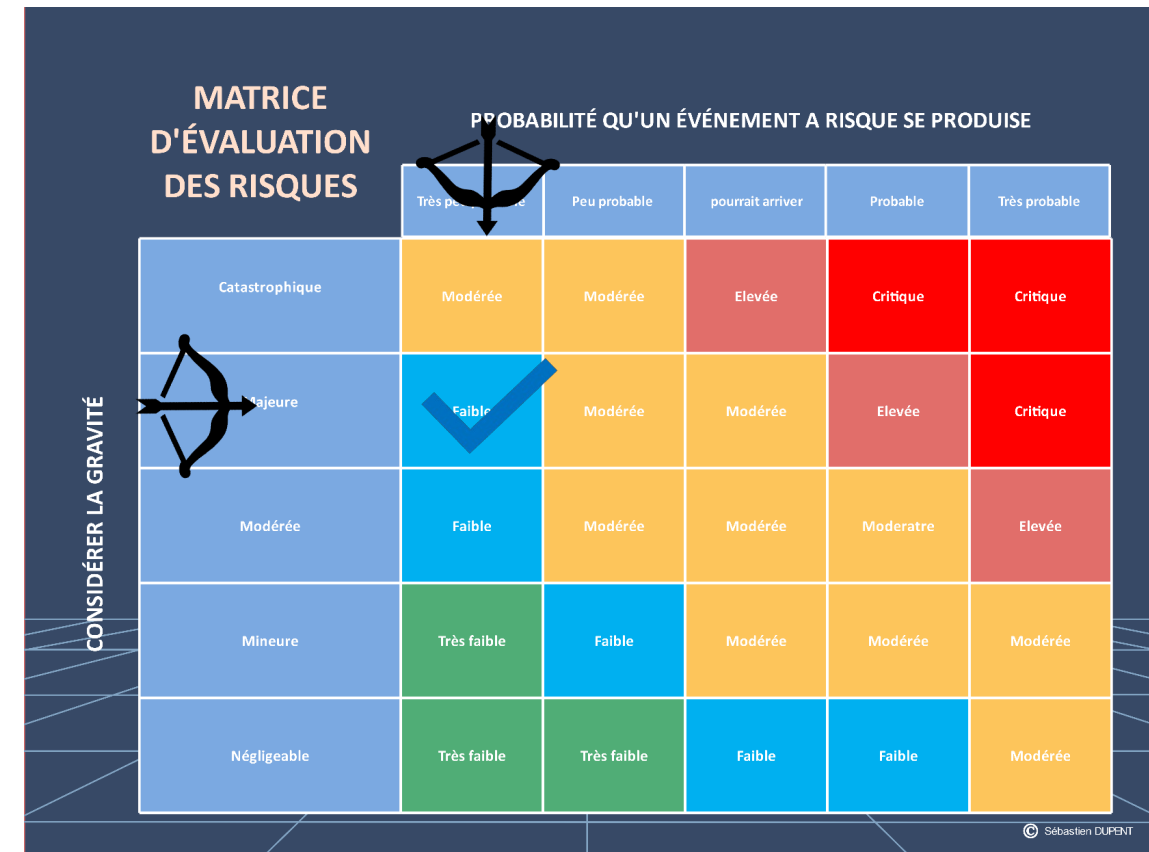
# Exemple

En résumé, **ne vous fiez pas** aux apparences d'un port USB car il pourrait bien « cacher des choses ». Il s'agit d'un système qui collecte les données des appareils auxquels il est connecté, peu importe les raisons. C'est une source d'énergie bancale, tel un puissant condensateur ou un ordinateur qui installe une porte dérobée sur votre appareil. Une chose que vous ignorez jusqu'à ce que vous le branchiez.

Quand on connecte son **smartphone** sur un **port USB**, l'appareil peut à la fois **se recharger**, mais aussi **transférer des données**. Le problème, c'est qu'il n'existe pas de réelle frontière entre les deux technologies : il est donc possible de dérober les données d'un smartphone, alors que l'utilisateur pense simplement recharger son téléphone. Le **juice jacking** fait partie de ces cyberattaques trop souvent ignorées, mais qui peuvent se révéler extrêmement malveillantes pour les victimes. Cette **méthode de piratage** consiste à récupérer les données d'un utilisateur qui pense innocemment recharger son smartphone sur une borne publique, comme on en trouve à foison dans les aéroports, les salons, les restaurants, etc.

## Insertion sur un des port USB d'un serveur un matériel externe à l'entreprise

- Fréquence possible minimum de moins d'une fois par mois (seulement quand on intervient sur le serveur) : Très peu probable
- Risque : Majeure



# Classification

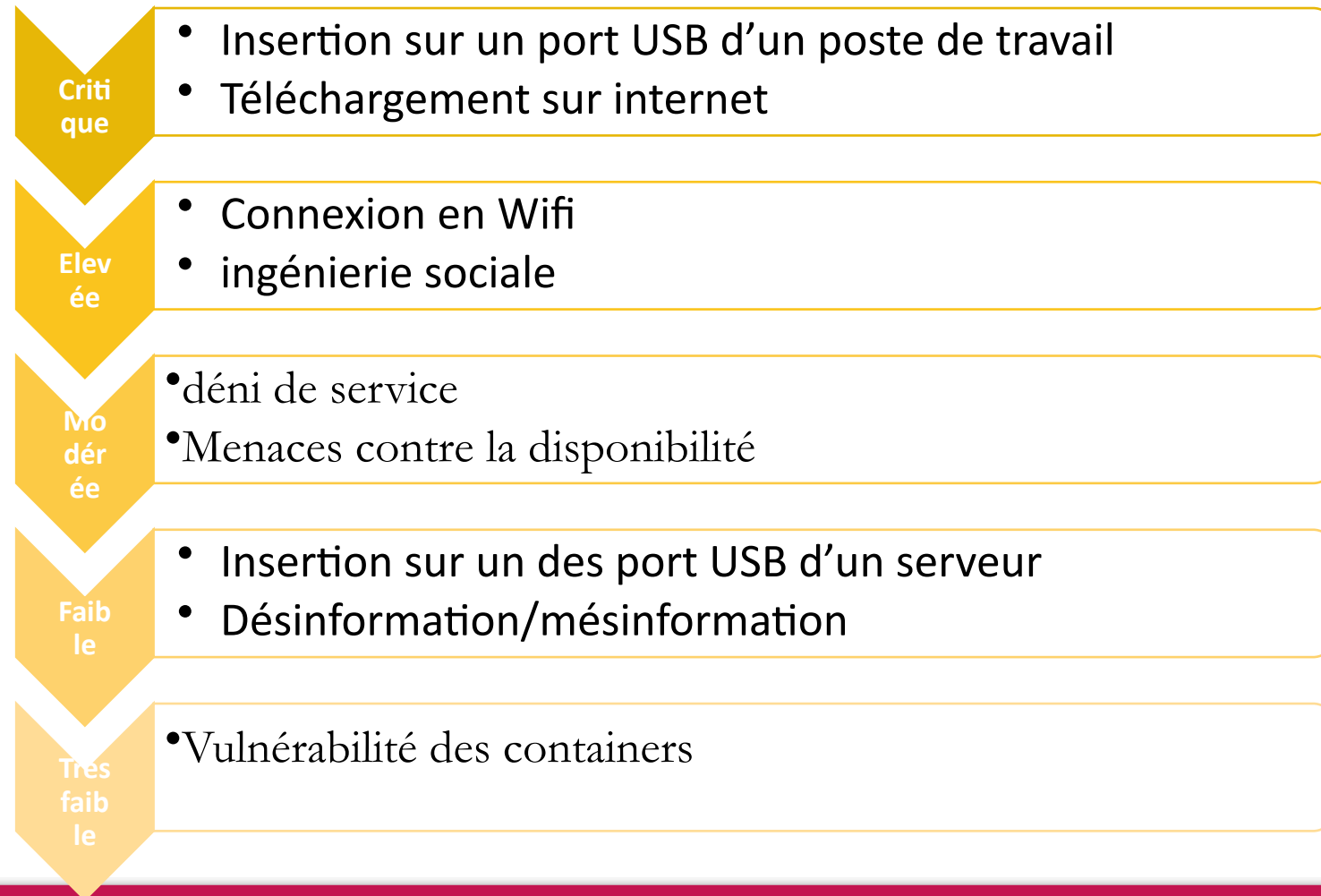


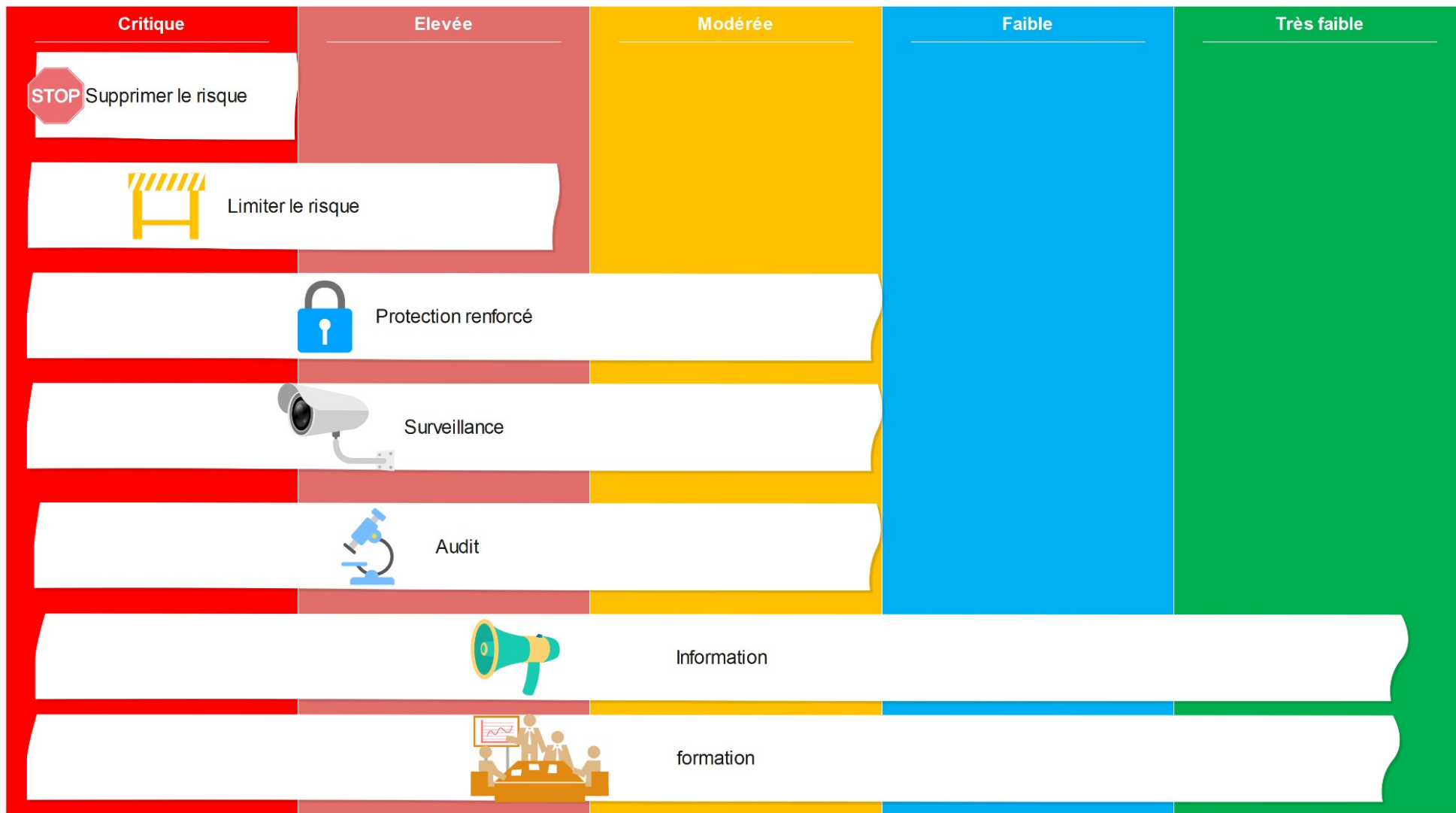
## Attention

ce classement est un exemple

Chaque organisation aura un classement différent selon son environnement

Une fois chaque risque évalué on pourra alors classer les risques du plus élevés au moins élevés est ainsi avoir une cartographie des priorités et action à mener











# Mise en place d'actions concrètes liées à la protection des données - RGPD

Par Sélim-Alexandre ARRAD

La conformité RGPD,  
ce n'est pas qu'une posture. Il ne  
suffit pas d'avoir l'air en conformité,  
encore faut-il le prouver.



AFCDP

« Accountability »

# Avant-propos

- *La conformité globale d'un organisme sous l'empire du RGPD est à apprécier sur une temporalité allant du 27 avril 2016, date de son entrée en vigueur, à nos jours.*
- *La date du 25 mai 2018, soit son entrée en application, équivaut à la pleine application de ses dispositions notamment coercitives.*

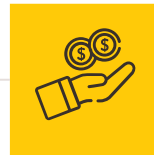
# SOMMAIRE

- *PLUS-VALUES DE L'INTÉGRATION DU RGPD*
- *GOVERNANCE PAR LES TEXTES*
- *LA DÉMARCHE DE CONFORMITÉ EN BREF*
- *FICHE DE TRAITEMENT, QUÉSACO ?*
- *DES DROITS ? QUELS DROITS ?*
- *SENSIBILISER ET FORMER SON PERSONNEL*

# PLUS-VALUES DE L'INTÉGRATION DU RGPD

## Gouvernance de votre organisation

Efficiences de vos processus « métiers » au service de votre performance

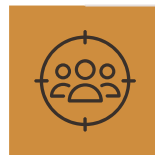


## Valorisation des données

Amélioration de votre efficacité commerciale

## Gage de confiance

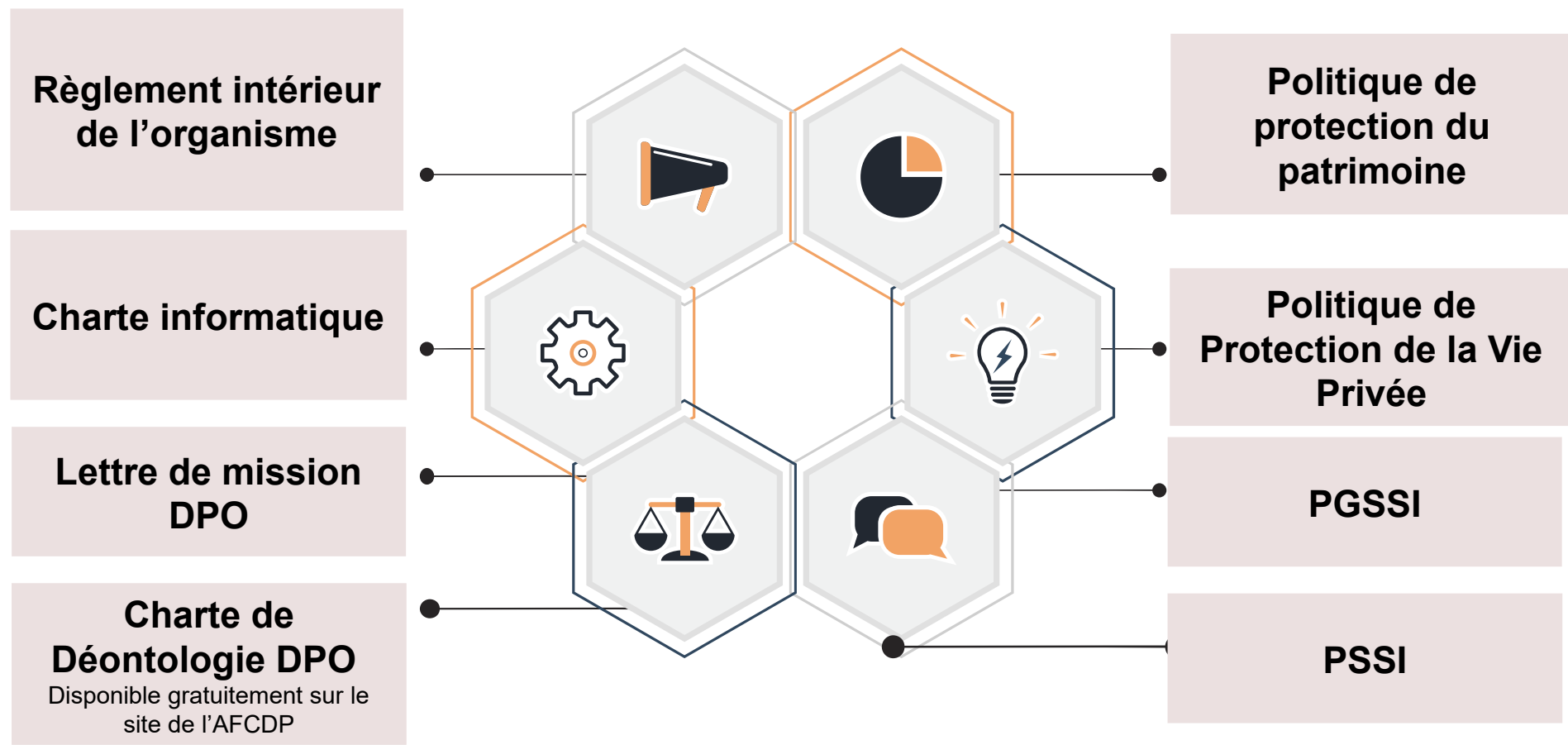
Replacer vos clients au centre de vos préoccupations



## Levier de compétitivité

Un avantage concurrentiel non-négligeable

# GOVERNANCE PAR LES TEXTES



# Démarche de conformité en bref

## Phase introductive

1

- **Sensibilisation RGPD** par direction et leurs chefferies de service

## Phase d'engagement

2

- **Détermination et point de contact dans les services**

3

- **Cartographie** des traitements via l'outil *ad hoc*

4

- **Analyse des traitements** et échange entre la DPD et son réseau

5

- **Constitution** des fiches de traitement

6

- **Analyse** des écarts

7

- **Présentation** du plan d'action

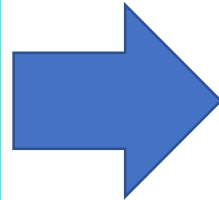
8

- **Suivi du plan d'action** et indicateur du **contrôle continu**

# FICHE DE TRAITEMENT, QUÉSACO ?

## Inscription au registre des traitements des organismes

- Participe à attester de la conformité au RGPD
- **Tenue d'une documentation complète obligatoire** : joindre à la déclaration tout document justifiant le respect du RGPD (*accountability*)
- Doit être réalisée **avant** la mise en œuvre du traitement
- **Le contenu doit être mis à jour en cas de changement dans le traitement**



## Contenu du formulaire de déclaration

Contexte, finalités du traitement et date de recueil

Personnes concernées par le traitement

Type de données traitées (recueillies, exploitées,...)

Destinataires des données et transferts hors UE

Recueil du consentement/Autre base légale


Information des personnes

Durée de conservation des données

Mesures de sécurité




# Des droits ?

 **Pleine compétence de la DPD pour instruire et répondre aux demandes.**

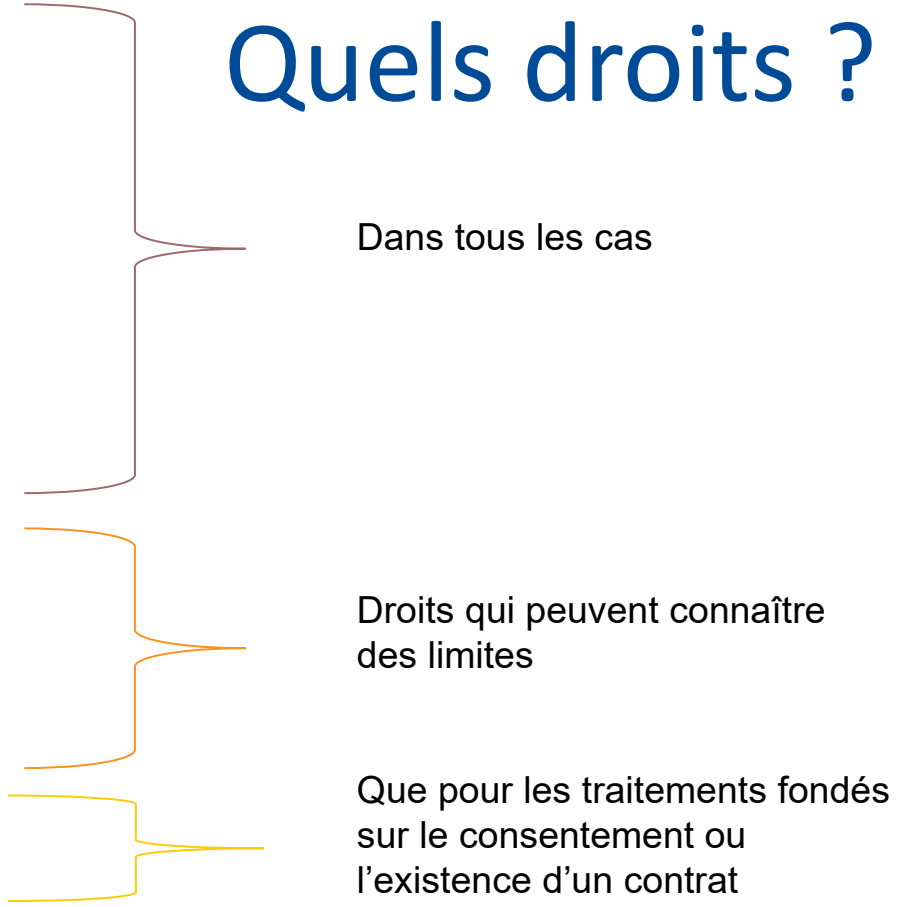
Exceptions pour :

- les demandes RH ;
- Infolettres si lien désinscription

 **1 mois pour répondre en principe**

- Droit d'information
- Droit d'accès
- Droit de rectification
- Droit à la limitation
- Droit d'effacement
- Droit d'opposition
- Droit à la portabilité

# Quels droits ?



**Droit d'introduire une réclamation auprès de la CNIL :** la **personne concernée** peut introduire une réclamation auprès de la CNIL, si elle estime que ses droits informatique et libertés ne sont pas respectés

# Sensibiliser et former son personnel



<https://atelier-rgpd.cnil.fr/login/index.php>

<https://secnumacademie.gouv.fr/>



**Le jeu inventé par l'Association française des Correspondants à la Protection des Données (AFCDP) et disponible pour les organismes souhaitant mener une approche « serious game » au sein de leurs entités.**



# Facteur humain et engagement des collaborateurs

Par Marion PIERRE et Denis MATHIS

*Cybersécurité :*

De l'importance de la  
prise en compte du  
**facteur humain**



**butachimie**  
Site de  
**Chalampé**

Créé en 1974  
125 hectares



## 2 ingrédients indispensables à **la fabrication du Nylon 6.6**

**ADN**

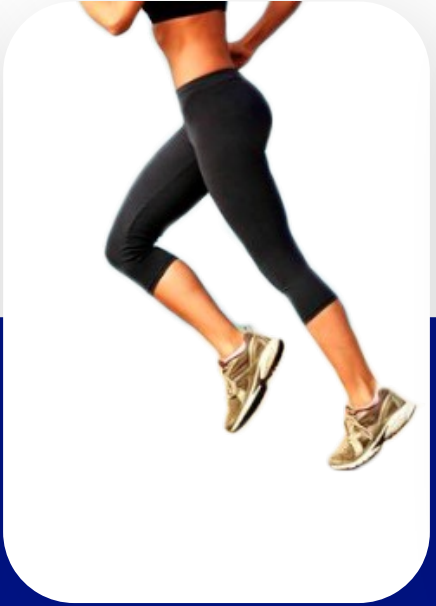
**Adiponitrile**



**HMD**

**Hexaméthylènediamine**

# A quoi sert le nylon 6.6 ?



# Unique site européen

de production d'ADN

**Nous disposons  
des deux  
meilleures  
technologies  
de fabrication au  
monde**



**25%**  
capacité  
mondiale  
d'ADN



# Une conscience accrue aux dangers

## Risques liés aux produits



**Toxique**



**Inflammable**

## Risques liés au procédé



**Pression  
>12b**



**Température  
>1100°C**

## Risques liés à la sûreté



**Vol de données  
dont IP**



**Terrorisme ou  
malveillance**

# Site Seveso seuil haut Obligation de se protéger !

# Préserver nos données et **notre propriété intellectuelle**

*Une nécessité « vitale » dans un  
contexte de compétition intense*

# Des attaques informatiques incessantes



**Chaque jour est marqué  
par une attaque**

**29 août 2023 : plus de 100 attaques en 1 jour**

→ **mai 2022 : 10 000 attaques sur deux journées consécutives !**

# Comment nous en protégeons-nous ?

Grâce à des barrières techniques multiples et

- **Coffre-fort électronique**
- **VPN**
- **Pare-feu**
- **Antivirus**
- **Authentification forte**

- **Sauvegarde et mises à jour régulières planifiées par l'Informatique**

- **Gestion des accès :**  
habilitation,  
exception,  
révocation, etc.

- **Stockage sécurisé :**  
armoires à clés  
et coffres-forts

- **Protection des ports USB**

- **Chiffrement des contenus sur nos GED**  
(ex : IRM)

- **Contrôle et reporting des mouvements de documents**  
(ex : DigitalGuardian)

- **Destruction sécurisée par broyeurs, bennes à papier sécurisées**

**Mais ces barrières ne sont pas infranchissables...**

Aussi performantes soient-elles, les barrières techniques  
**peuvent être contournées ou percées**

... Reste à évoquer un élément notable du système :

**le facteur humain**

Si la contribution  
**de l'humain**

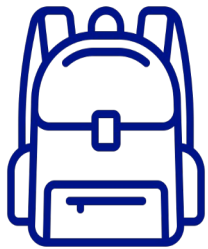
*à la sécurité est d'abord*

**positive**

L'humain peut aussi être  
**facteur de faillibilité**

# Trois petites histoires à méditer

Le sac et  
la voiture



La clé  
infectée

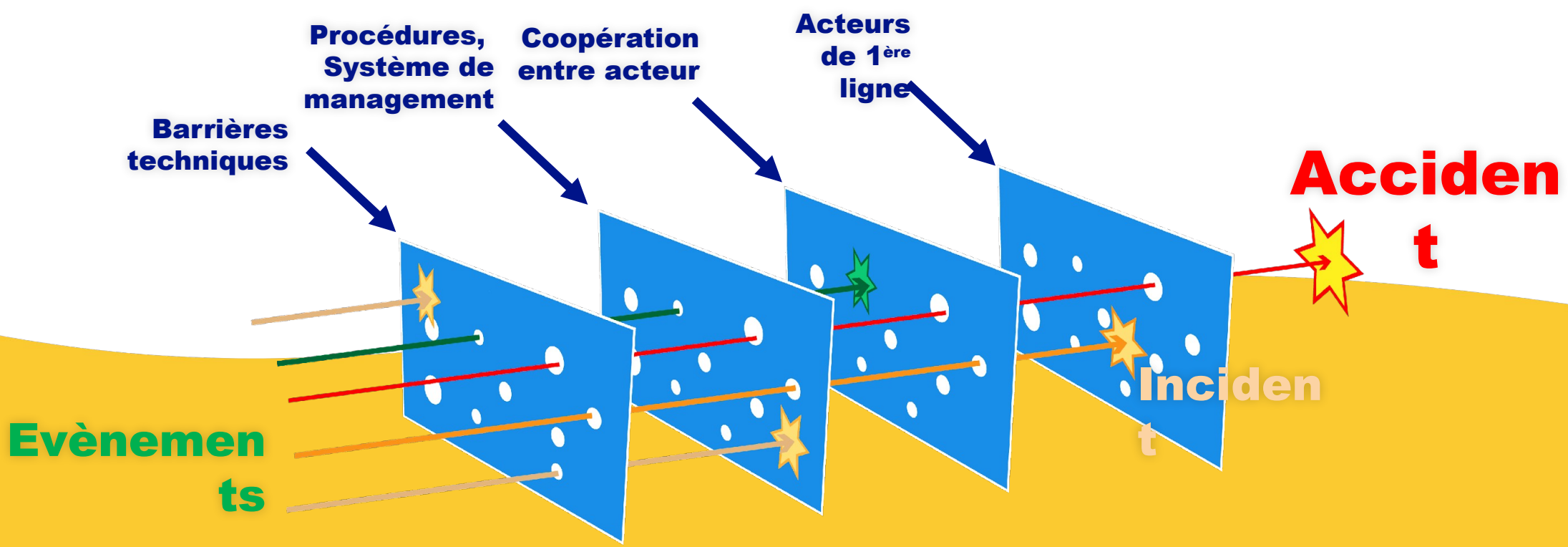


Vire-moi ton  
salaire



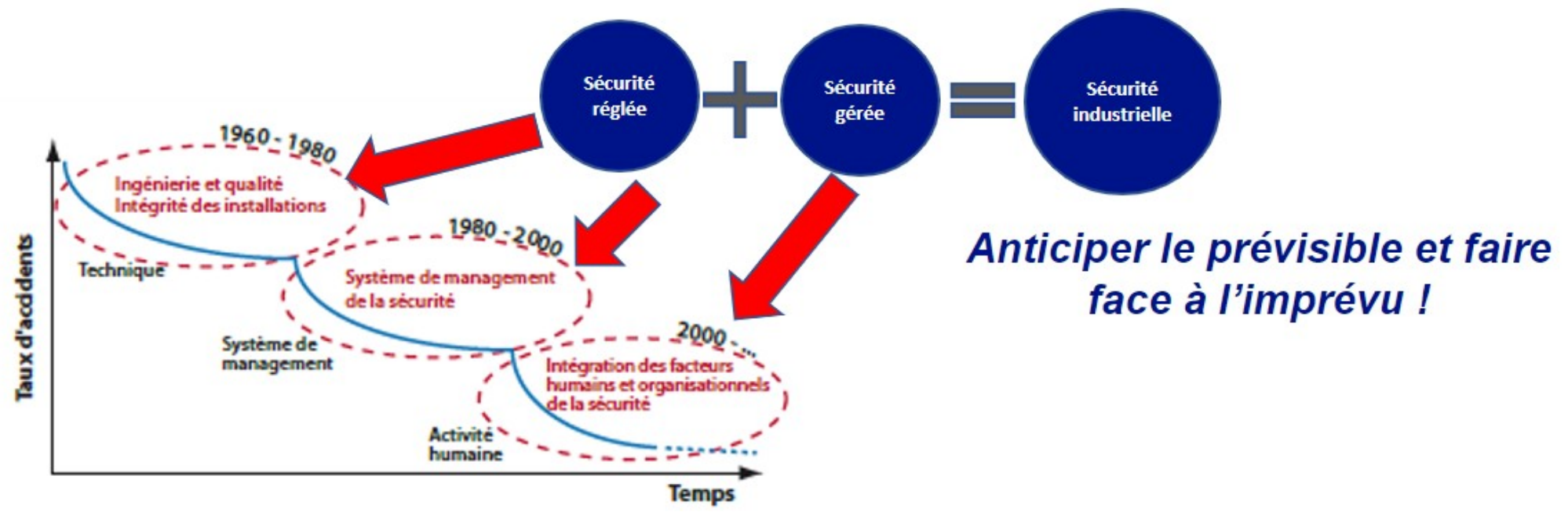
# S'inspirer de la sécurité industrielle pour protéger la sûreté de nos données

Le modèle du "fromage suisse", de James Reason

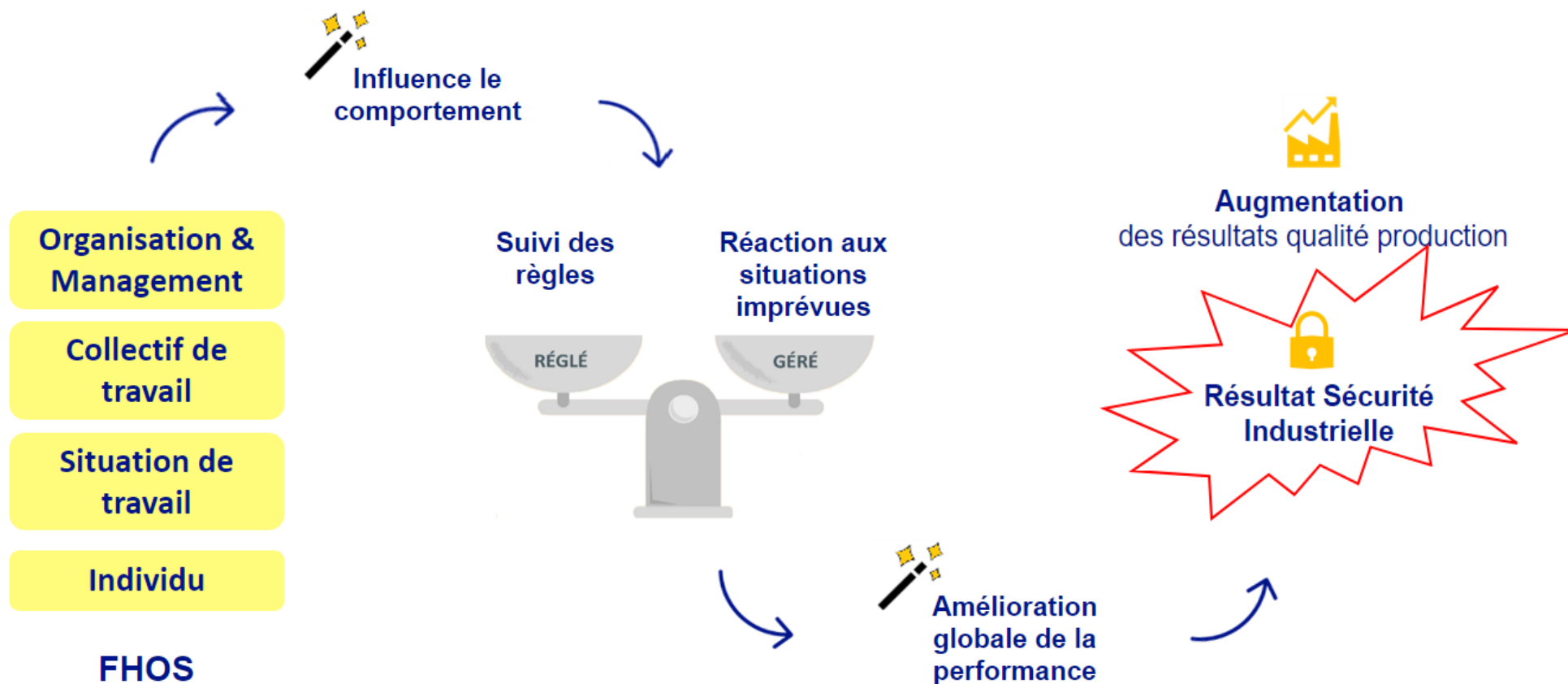




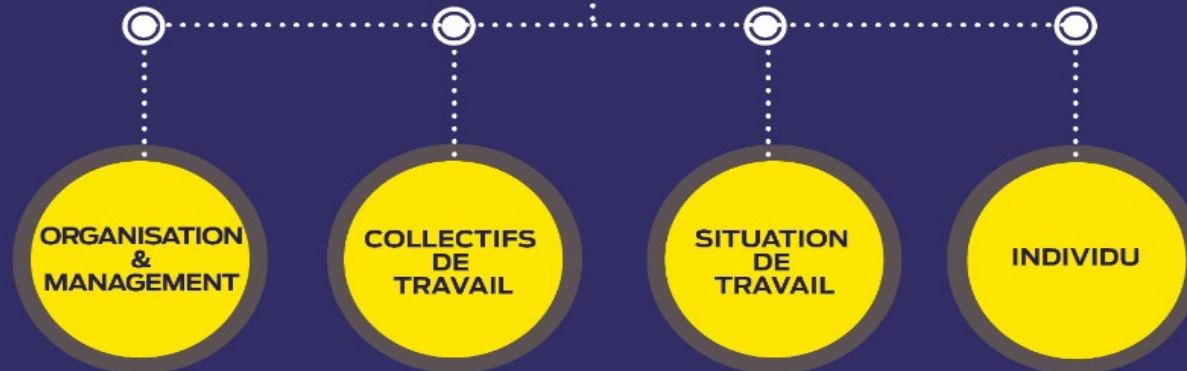
# Le facteur humain *un élément de progrès*



# Les facteurs humains et organisationnels de la sécurité industrielle (FHOS)



# les FHOS comme leviers du renforcement de la cybersécurité



- Engagement Direction
- Charte SI & PI
- Processus PI
- Procédures classification
- NDA
- Plan de restauration data

- Valeurs sécurité
- Vigilance partagée

- Audits
- Faux e-mails de phishing
- QCM
- Journée Sécurité
- Journée de la PI

- Formation
- Page web et vidéos
- Ecran de veille didactique



**Merci de votre  
attention**

 **butachimie**





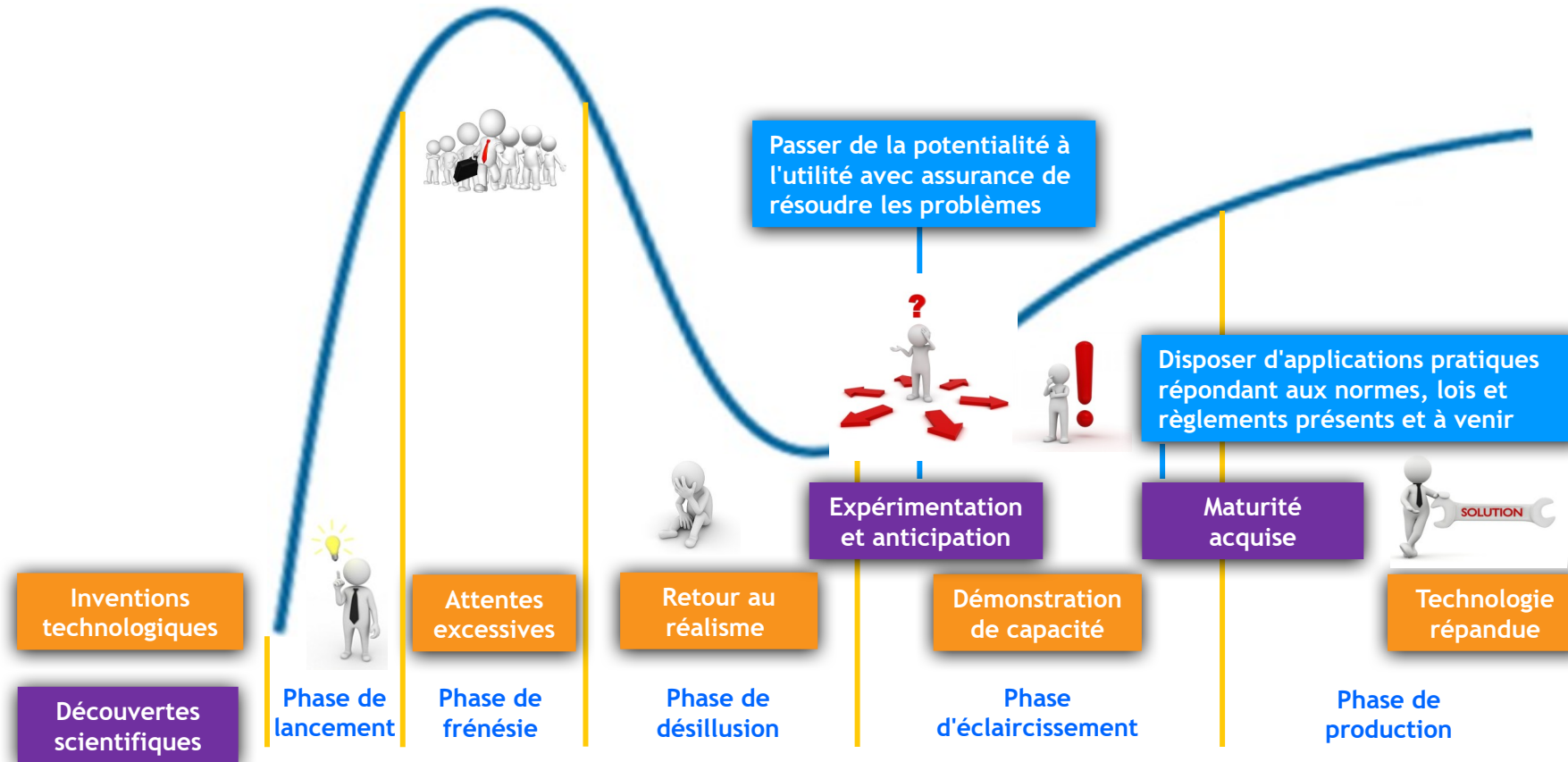
Nos observateurs spéciaux

Le retour...

# Conférence de clôture

## Prospective : Intelligence Artificielle, cybersécurité versus cybercriminalité

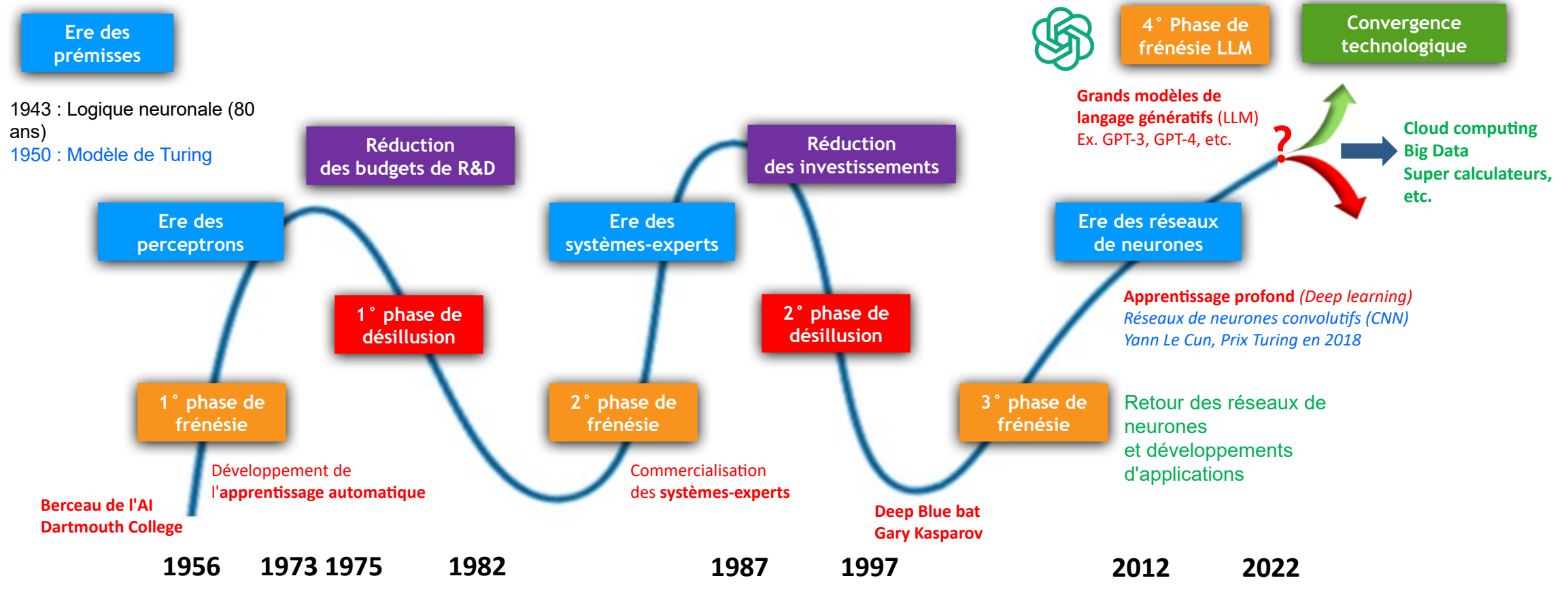
Par Daniel GUINIER  
Colonel (RC) de la Gendarmerie Nationale



Courbe "hype" de l'évolution de l'intérêt pour une technologie nouvelle en fonction du temps dans un cheminement : sciences-technologies-innovations.

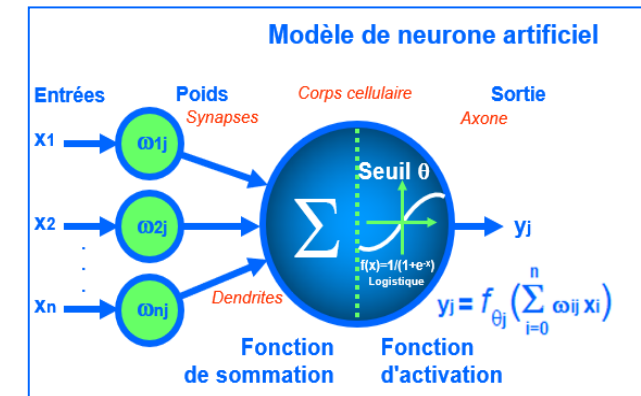
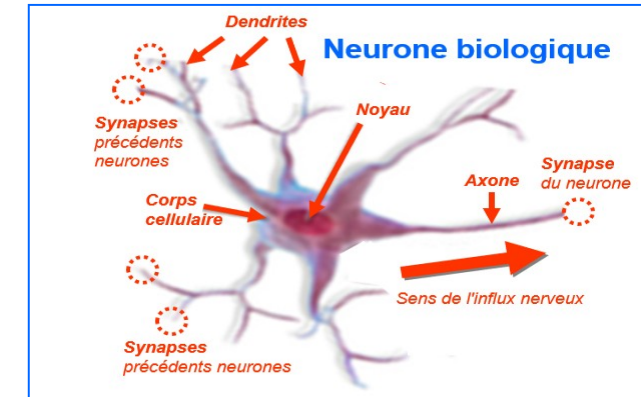
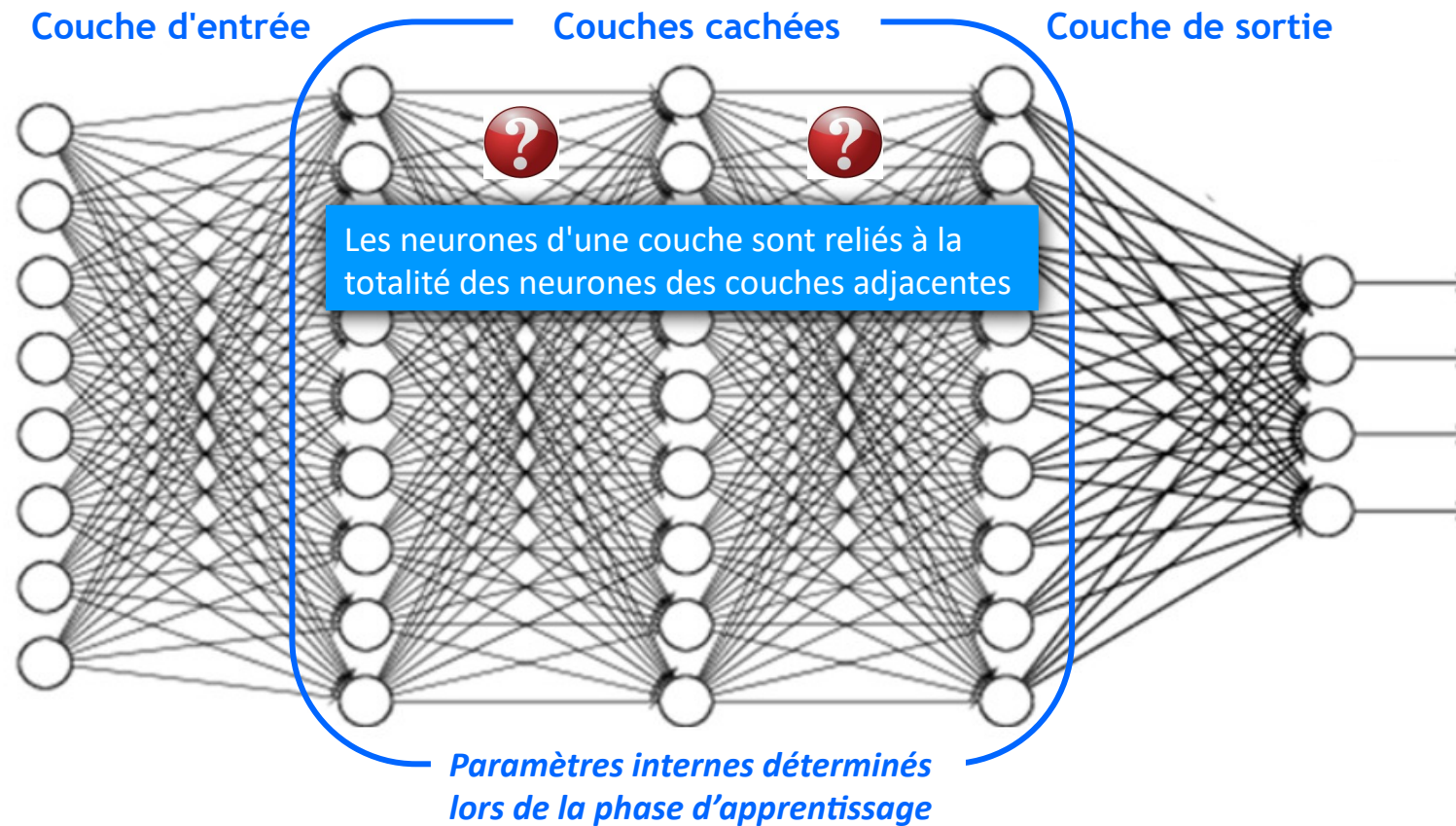


# L'odyssée de l'intelligence artificielle (IA)

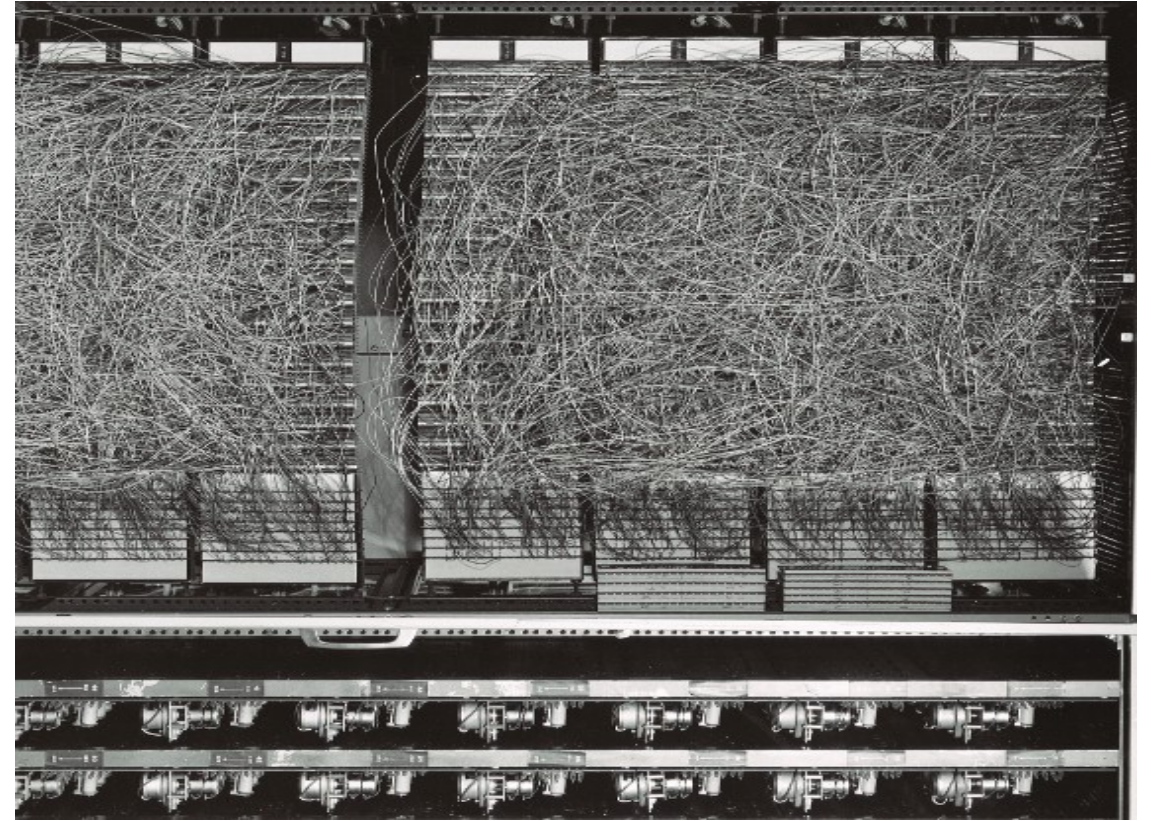
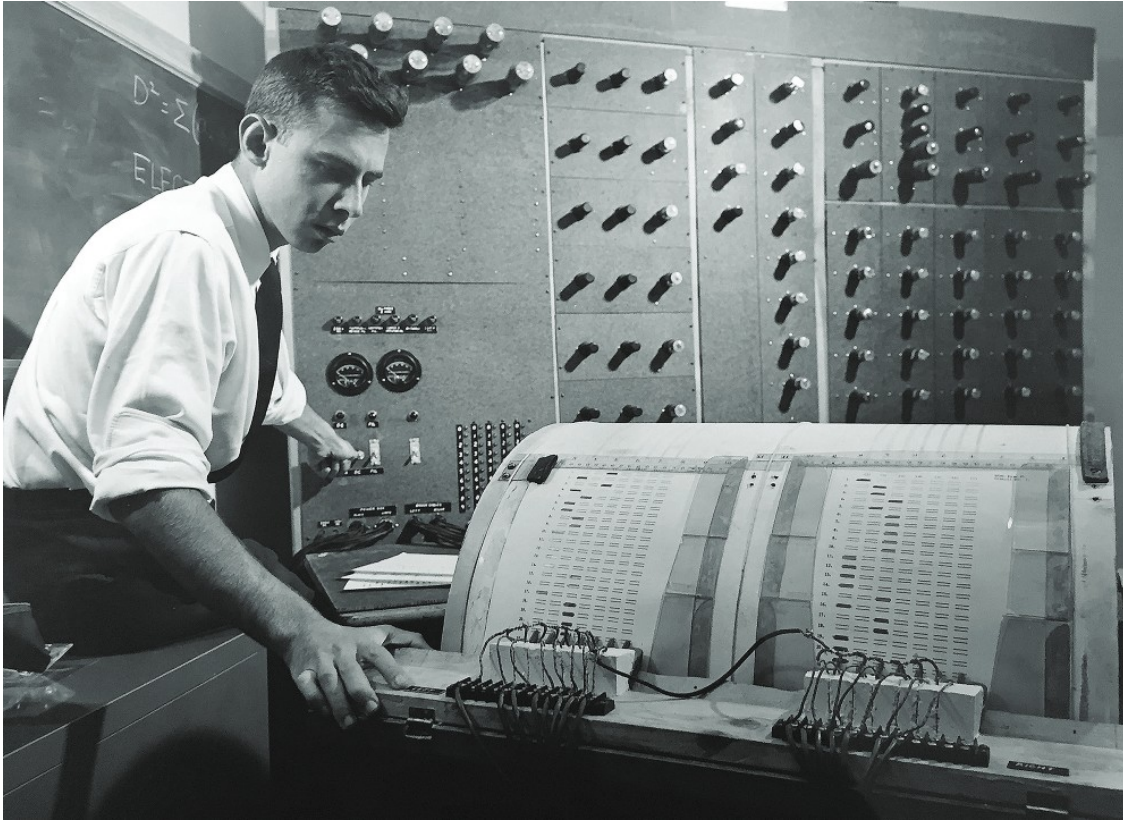


1956 : Dénomination "intelligence artificielle"  
1957 : Construction du perceptron Mark I  
1965 : Premier système-expert

Cheminement de l'IA par vagues successives depuis l'origine, passant par plusieurs phases de frénésie et de désillusion, influencées par le symbolisme et le connexionnisme, sur 80 ans après les prémisses.



McCulloch et Pitts (1943)



Si le **Perceptron Mark I**, inventé par Frank Rosenblatt en 1957 puis construit au laboratoire d'aéronautique de Cornell, a été présenté comme **"le premier dispositif capable de penser comme le cerveau humain"**, ce qui est très exagéré et a été amplifié par le battage médiatique.

Le perceptron n'est qu'un réseau de neurones simple disposant de la capacité de séparer deux classes après un apprentissage supervisé.

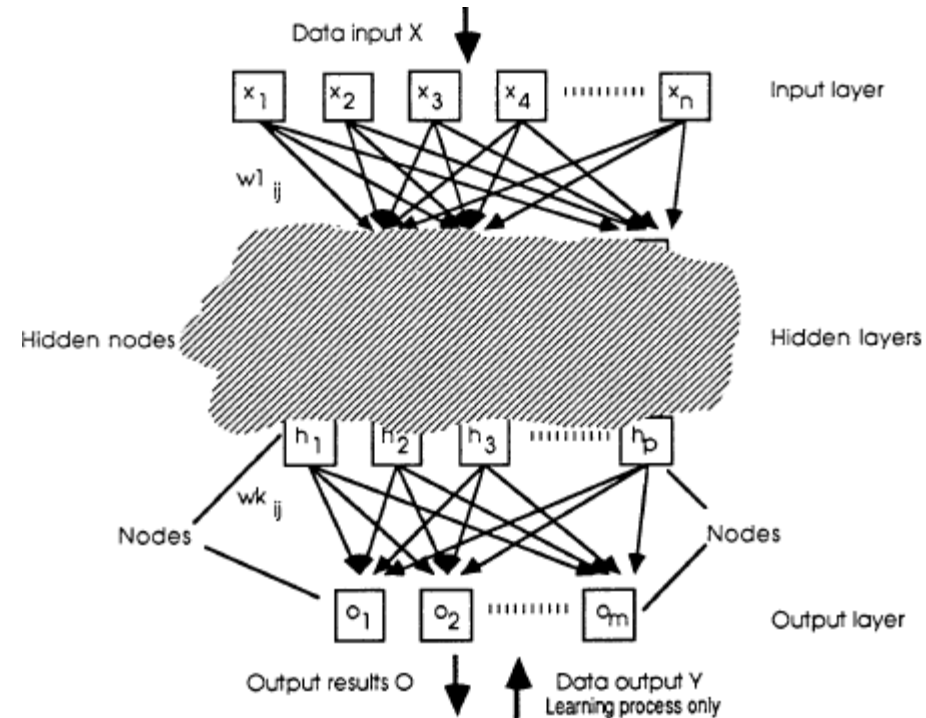
## Abstract

**Computer viruses** are more and more numerous : around 400 in the year 1990 and this number is estimated to reach 1,000 for 1994-95. Users are not experts and need help in identifying the virus and carrying out the most appropriate cure in case of attack.

**Knowledge** of viruses is necessary but public information offered by virus databases or catalogues give a powerful advantage to virus makers. On the other hand, not enough or no information to users is also a problem because then they use the product, they have which does not necessarily provide the appropriate solution in case of virus attack. We propose **an alternative solution to the dilemma found in a neural network**, an artificial intelligence connectionist model, which is fault tolerant, self adaptative to learn automatically, retaining experience to solve the problem of virus identification regarding **fuzzy information** on concerns and effects.

Principles of the formal neuron and the **neural network using hidden nodes** is examined as well as the theoretical and practical aspects of the **gradient back propagation algorithm**. An **implementation of the algorithm** is applied to **virus identification** with data referring to virus concerns and their obvious effects. First results have shown a correct **identification of viruses** while using fuzzy knowledge of end users introducing uncertainty on answers or, even, forcing erroneous data. Such a system can be employed by ordinary users, system or computer security managers, as well as consultants as a complementary **tool for virus warfare**.

Further work needs to be conducted to validate methodologically such an approach and to optimize input data coding, the choice for parameters and the learning strategy.



Guinier D. (1991) : Computer "virus" identification by neural networks. *An artificial intelligence connectionist implementation naturally made to work with fuzzy information*. ACM SIGSAC Review, vol. 9, n°4, pp. 49-59.  
*Référence scientifique du brevet : Patent US 5,511,163 déposé par M. Lerche (DK) et C. Howitz (DK) en 1996.*

De 1990 à 2020 on relève l'apparition de plus d'un milliard de codes malveillants.

Première validation de l'efficacité d'un réseau de neurones artificiels dédié à l'identification des virus informatiques après apprentissage automatique.

## □ Phase lente d'apprentissage à partir d'un échantillon de données

- Faire correspondre un ensemble d'entrées à une sortie en ajustant les paramètres
  - Mode supervisé : *Détermination d'une fonction de prédiction à partir de données étiquetées manuellement*
  - Mode non supervisé : *Détermination autonome de structures sous-jacentes aux données non étiquetées*
- Propagation du signal depuis l'entrée vers la sortie et rétropropagation de l'erreur depuis la sortie
- Détermination des poids des connexions entre neurones visant à minimiser l'erreur de sortie

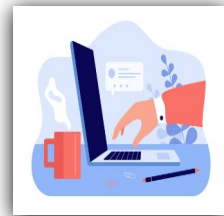
## □ Phase rapide opérationnelle

- Soumission de données d'entrées au réseau ayant appris
- Récupération des résultats de sortie

Lors de l'apprentissage, le réseau effectue un calcul de proche en proche, pour déterminer une valeur de sortie. L'erreur est calculée au niveau de chacune des connexions de sortie, pour être ensuite rétro-propagée dans le réseau pour modifier chaque poids. L'opération est répétée jusqu'à ce que l'erreur soit inférieure à un seuil maximal choisi. A ce moment le système est réputé opérationnel.

Le Grand Modèle de Langage (LLM) GPT-3 d'OpenAI, a été entraîné en 2021 sur 300 milliards de mots pour cerner le langage naturel et l'interpréter avec 175 milliards de paramètres, pour fournir des réponses contextualisées fondées sur son architecture de transformateur génératif pré-entraîné.

**Entrée** : Demande sous forme d'une séquence de texte (GPT-3) et multimodale (GPT-4)

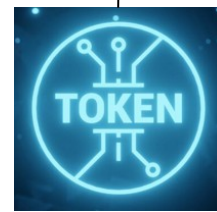


**Prétraitement** : Nettoyage et normalisation de la séquence



Texte simplifié au maximum mais gardant tout son sens

**Division** : en unités lexicales (*jetons*) pour faciliter la compréhension

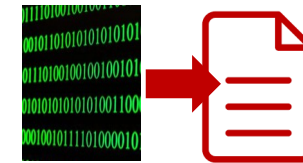


Max. 4096 jetons avec GPT-3.5

**Encodage** : Les jetons sont convertis en valeurs numériques pour être traités par le modèle LLM



**Décodage** : Le modèle prédit par probabilité la prochaine séquence cohérente en fonction du contexte de la demande.



**Sortie** : La réponse fournie est entièrement satisfaisante ou nécessite un nouveau cycle



**Raffinement** : Boucle de rétroaction pour obtenir des informations complémentaires ou une meilleure qualité de réponse

© 2023 D. Guinier

Le transformateur GPT (*Generative Pre-trained Transformer*), basé sur des mécanismes d'attention, dispose d'un mode d'apprentissage semi-supervisé faisant appel à une représentation, qu'il adapte en fonction du contexte à l'aide du modèle dynamique de langage appris.

## □ Dans la connaissance et la gestion des menaces

*Alliance des analystes humains avec l'IA partie prenante capable d'apprendre*

- Aide à la cartographie des données collectées et nécessaires à l'activité
- Veille permanente concernant les actifs informationnels et les divers risques encourus
- Détection automatique de vulnérabilités et de menaces inconnues des organismes
- Renforcement des défenses essentielles (ex. *authentification forte par reconnaissance faciale*)
- Détermination des ressources et règles, au vu de nouveaux risques et ceux créés par l'IA générative, etc.



## □ Dans la détection et la réponse aux incidents

*Analyse plus efficace avec l'IA capable de traiter en continu de grands volumes*

- Distinction en temps réel entre les comportements normaux, illégitimes et subtiles (ex. *Attaques APT*)
- Détection des attaques masquées parmi d'innombrables incidents à traiter
- Analyse et hiérarchisation des alertes selon des critères appropriés (ex. *crédibilité, pertinence et gravité*)
- Aide à la coordination des réponses à apporter et soutien au centre opérationnel de sécurité (SOC)
- Possibilité de supervision de l'IA par le raisonnement humain, selon le contexte et les objectifs, etc.

### ❑ Dans les attaques visant les systèmes d'IA

- Modifications malveillantes de programmes d'IA
- Empoisonnement des données d'apprentissage

### ❑ Dans les attaques visant les organismes

- Offre de systèmes d'IA intentionnellement corrompus
- Hameçonnage exploitant des biais cognitifs optimisés pour la cible
- Atteinte à la réputation par des bots sociaux (*ex. en répandant rapidement des millions de messages sur Internet*)
- Usurpation d'identité et génération automatique de fausses informations (*ex. vidéos, articles, messages, etc.*)

### ❑ Dans les créations par IA en vue d'attaques

- Réalisation automatique de logiciels malveillants, notamment en vue d'attaques subtiles
- Découverte de failles techniques et humaines et offres sur les *Darknets*
- Génération de *spams* personnalisés crédibles et de *deepfakes* difficilement détectables (*ex. FakeCatcher*)
- Génération de botnets intelligents pilotés par IA, etc.





## ❑ Premier paradoxe avec l'IA

- L'IA est favorable à la cybersécurité, apportant son aide et palliant certaines limites humaines
- L'IA est favorable aux cybercriminels, leur donnant des facilités pour la production et la subtilité des attaques

## ❑ Second paradoxe avec l'IA

- Des compétences humaines de haut niveau sont nécessaires pour disposer d'un temps d'avance
- Ces compétences manquent cruellement ou au mieux sont insuffisantes

## ❑ Pour l'Etat, la bataille pour la souveraineté est engagée

- Initiation d'une stratégie IA en 2018, création du comité de l'IA en sept. 2023 pour un rapport dans 6 mois
- Une filière nationale de l'IA est à développer, et une réglementation et une certification sont attendues

## ❑ Pour les organismes, la nouvelle donne est à intégrer

- Evaluation des risques et la façon de les limiter au vu des nouvelles menaces, y compris celles de l'IA générative
- Estimation des avantages de l'IA en vue de son adoption, après étude et expérimentation

# Merci de votre attention



DG

*"En fait, qui es-tu ChatGPT ?"*



*"Je suis un modèle de langage développé par OpenAI. Mon objectif est d'aider à fournir des réponses, des informations et une assistance dans divers domaines en fonction des questions et des sujets qui me sont présentés..."*





Nos observateurs  
toujours aussi spéciaux

# Conclusion du 16<sup>ème</sup> FRC

**par le général Jude VINOT**

Commandant le Groupement de Gendarmerie Départementale du Bas-Rhin

**par Gilbert GOZLAN**

Col (RC) Gendarmerie Nationale

Président de l'association Ad honores – Réseau Alsace

# FRC 2023 - Remerciements

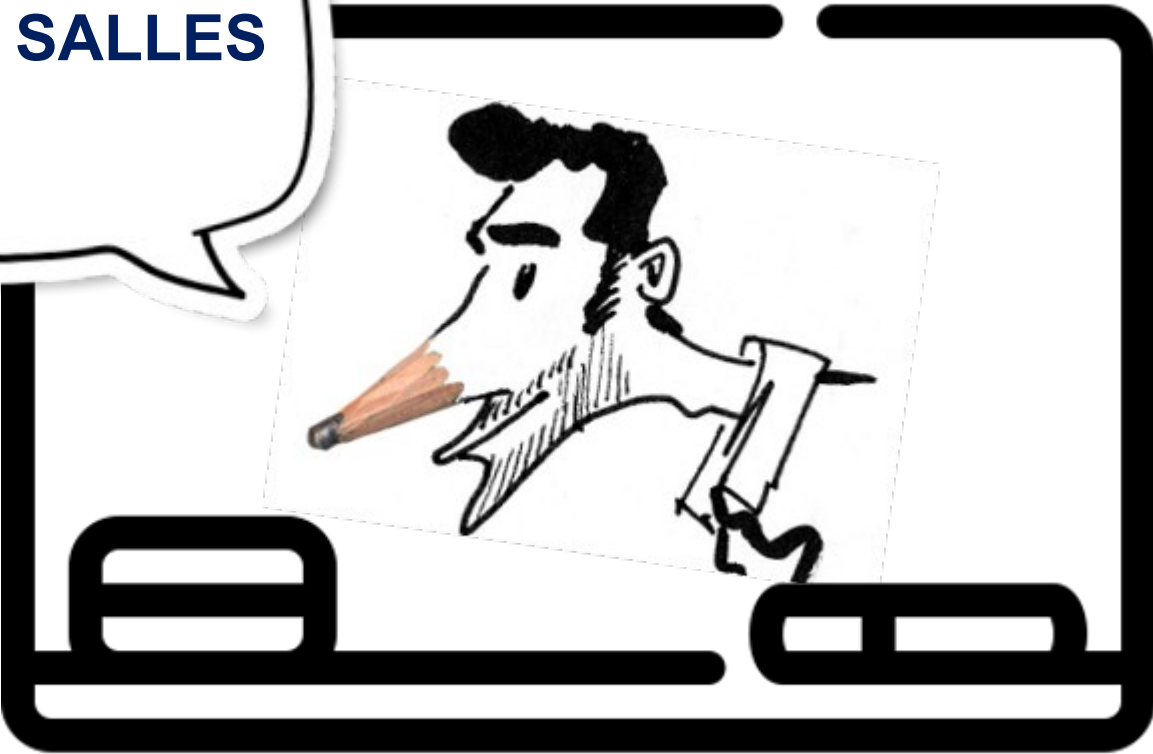
## L'équipe d'organisation

CEN Gérald DULOISY  
Sébastien DUPENT  
Daniel GUINIER  
Gilbert GOZLAN  
Joël GUERET  
Emmanuelle HAASER  
Hervé HUMBERT

Sophie MARTIN  
CNE Andrée NTORE-BIKENE  
Didier SCHERRER  
MDC Vanessa URBAN  
ADJ Eléna VALLEJO  
Jonathan WEBER



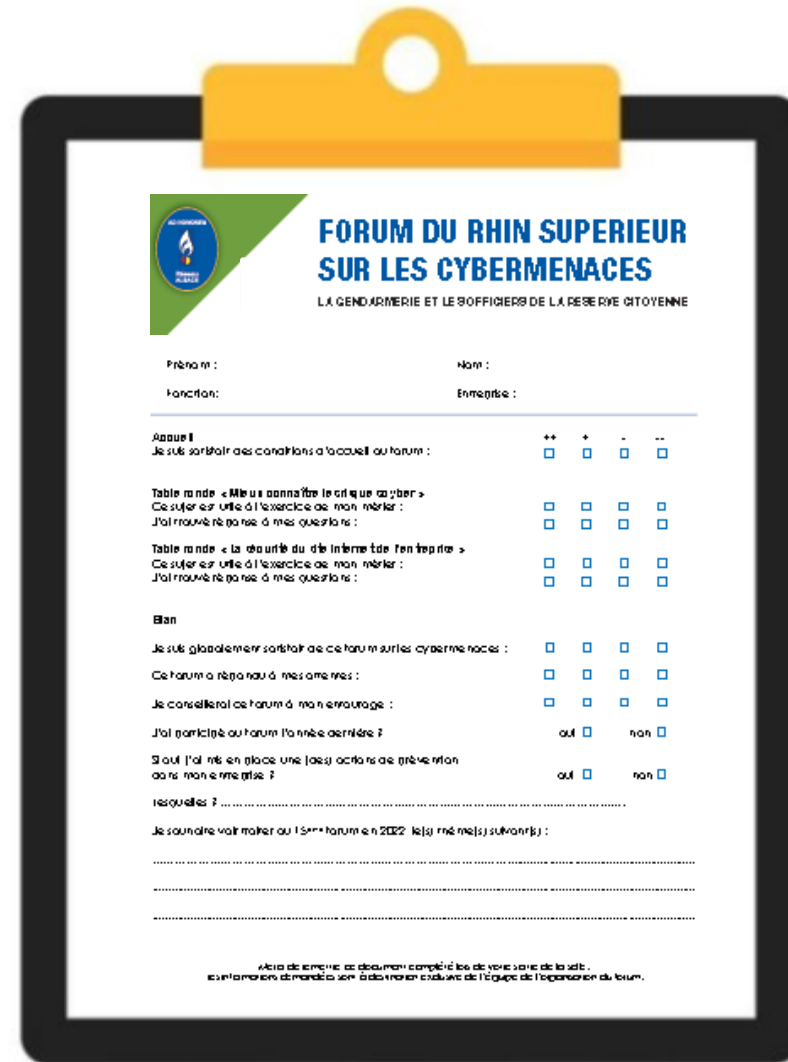
Laurent SALLES






**Marko MAYERL**  
**Camille COMPARON**

**Inédit Théâtre**





## FORUM DU RHIN SUPERIEUR SUR LES CYBERMENACES

LA GENDARMERIE ET LES OFFICIERS DE LA RESERVE CITOYENNE

Prénom : \_\_\_\_\_ Nom : \_\_\_\_\_  
 Fonction : \_\_\_\_\_ Entreprise : \_\_\_\_\_

**Accueil**  
 Je suis satisfait des conditions d'accueil au forum :      ++    +    -    --

**Table ronde « Meilleure connaissance de ce que c'est cyber »**  
 Ce sujet est utile à l'exercice de mon métier :                    
 J'ai trouvé réponse à mes questions :

**Table ronde « La sécurité du site Internet de l'entreprise »**  
 Ce sujet est utile à l'exercice de mon métier :                    
 J'ai trouvé réponse à mes questions :

**Bilan**

Je suis globalement satisfait de ce forum sur les cybermenaces :                    
 Ce forum a répondu à mes attentes :                    
 Je conseillerai ce forum à mon entourage :                    
 J'ai participé au forum l'année dernière ?      oui     non   
 Si oui j'ai mis en place une (des) action(s) de prévention de mon entreprise ?      oui     non

Lesquelles ? .....

Je souhaite voir naître ou l'année prochaine 2022 la(s) thématique(s) suivante(s) :  
 .....  
 .....

Afin de garantir ce document complété de votre service de la sécurité, les informations demandées sont à destination exclusive de l'équipe de l'organisation du forum.



# FORUM INCYBER EUROPE



**26-28 MARS 2024**

**FORUM INCYBER 2024**

**Ready for AI?**

Rendez-vous pour la 16e édition du Forum  
InCyber à Lille Grand Palais

## 17 ème FRC : 5 novembre 2024

<https://adhonores.alsace/>

