RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ÉTAT DE LA MENACE CYBER

6ÈME JOURNÉES FRANCOPHONES DE BIOLOGIE MÉDICALE

12 octobre 2023

L'ANSSI

Agence nationale de la sécurité des systèmes d'information créée en 2009

Autorité nationale en matière de cybersécurité et de cyberdéfense

Service de la Première ministre rattaché au Secrétariat général de la défense et de la sécurité nationale (SGDSN)

Mission défensive (et non offensive)

Rôle : protéger la Nation face aux cyberattaques

Cibles : OIV (Opérateurs d'importance vitale), OSE (Opérateurs de services essentiels) et administrations

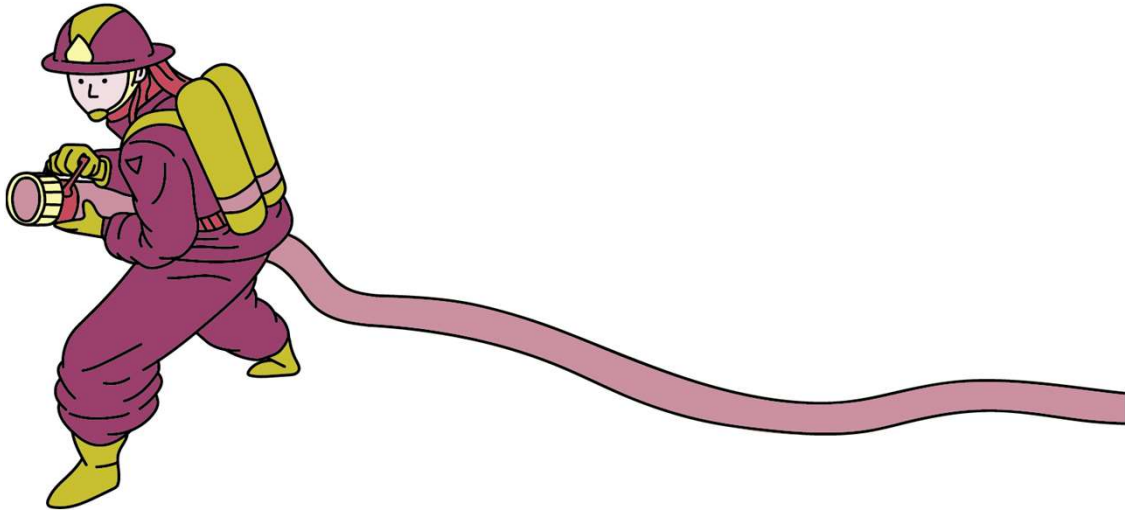
Cyber pompier…

En réponse à une menace qui se maintient à un niveau élevé.

Le gain financier, l'espionnage et la déstabilisation sont les principaux objectifs des attaquants.

L'ANSSI se doit de :

- Protéger les victimes de cyberattaques d'ampleur ;
- Défendre les systèmes d'information critiques de la Nation.



Quelques attaques ces derniers jours…

« La Cour pénale internationale victime d'un incident de sécurité »

« Le groupe de casinos MGM paralysé par une cyberattaque »

« La fédération néerlandaise de football paye une rançon à un cybergang »

À qui le tour ?

« L'assurance maladie des Philippines touchée par une cyberattaque »

« La ville de Morlaix victime d'un rançongiciel »

« Depuis ce week-end deux hôpitaux des Vosges sont retournés au papier, victimes d'une cyberattaque »

« La chaîne Pizza Hut victime d'une cyberattaque en Australie »

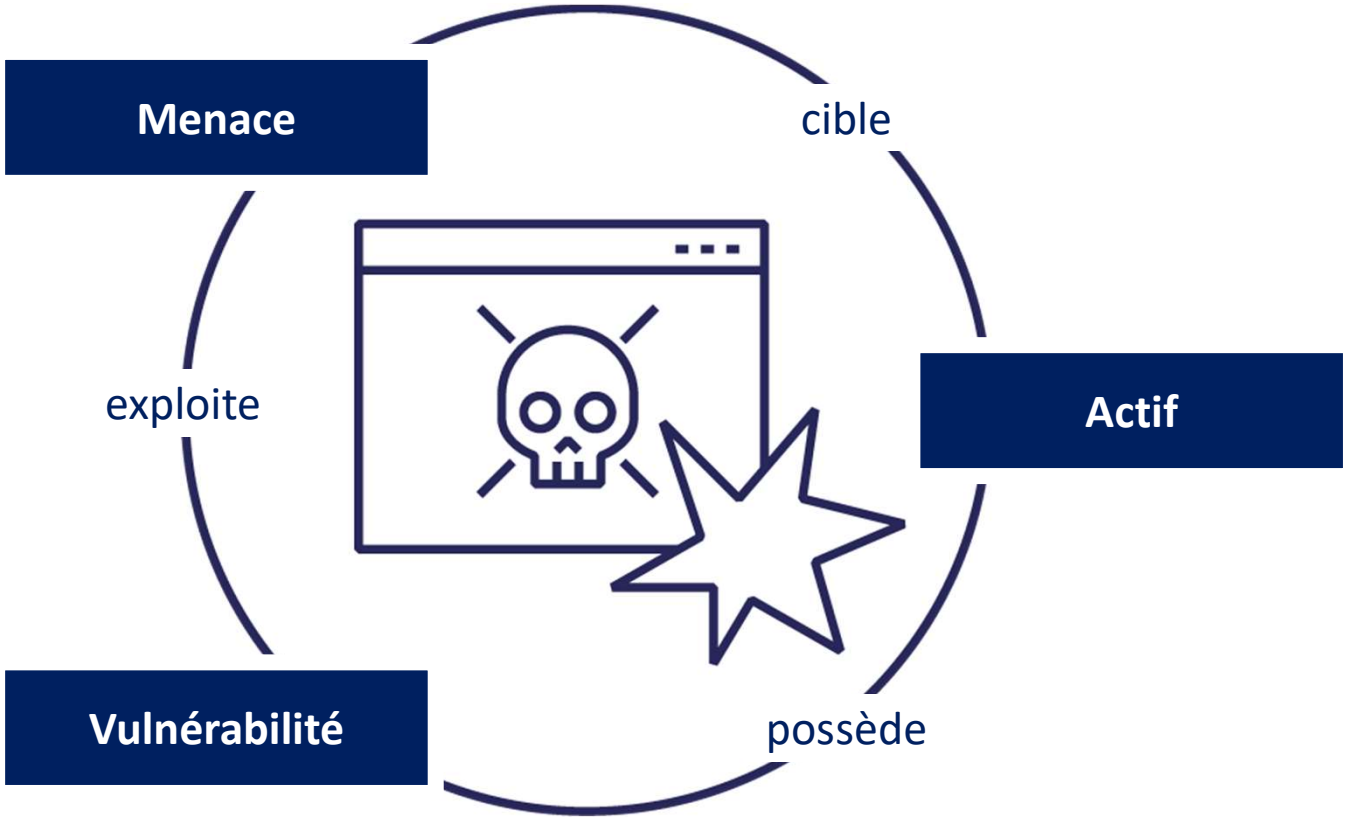
Le secteur santé n’est pas épargné

Quelques attaques marquantes :

- CHU de Rouen (2019)
- CH de Dax (2021)
- CH de Villefranche/Saône (2021)
- GHT Cœur Grand Est (2022)
- CH Sud Francilien (2022)
- CH de Versailles (2022)
- GHT de La Réunion (2023)
- CHU de Brest (2023)
- CHU de Rennes (2023)
- CHI Ouest Vosgien (2023)
- … ?

Illustration reproduite avec l’autorisation de Me Ledieu : https://technique-et-droit-du-numerique.fr/retex-de-la-cyber-attaque-contre-le-chu-de-brest-podcast-nolimitsecu-23-juillet-2023

Anatomie d’un incident de sécurité



Les acteurs de la menace

Menace cybercriminelle

- Groupes criminels
- Motivation : l'argent
- Attaques opportunistes, phénomène de masse, professionnalisation
- Rançongiciel, vol et vente de données personnelles

Menace stratégique

- Groupes étatiques ou financés par des États
- Motivation : espionnage, déstabilisation
- Attaques ciblées, furtivité
- Moyens techniques importants
- Espiogiciel, wiper, rançongiciel

Menace isolée

- Individus isolés : hacktivistes, employés mécontents, etc.
- Motivation : idéologie, exploit technique, vengeance, etc.
- Attaques ciblées
- Moyens plus limités
- DDoS, défiguration de site

Les vulnérabilités couramment observées

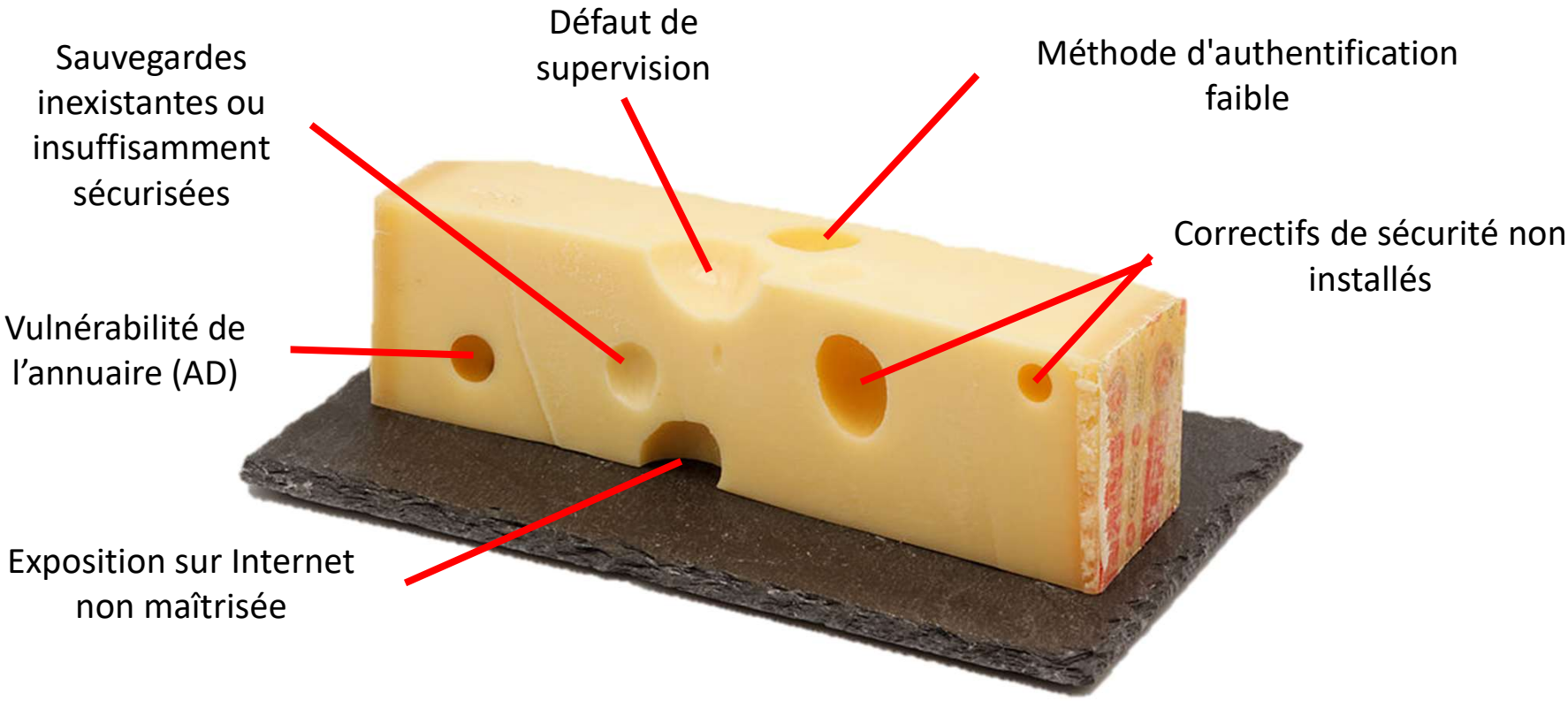


Illustration : https://commons.wikimedia.org/wiki/File:Emmental_(fromage)_01.jpg (licence Creative Commons)

Comment faire face à la crise : l'ANSSI et ses outils

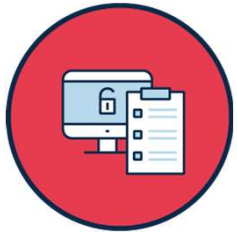
Collection gestion de crise cyber

La **collection « Gestion de crise cyber »** est destinée à accompagner les organisations dans la préparation et la gestion de crise cyber.
Trois guides en font partie :

- Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique
- Organiser un exercice de gestion de crise cyber
- Anticiper et gérer sa communication de crise cyber

Comment faire face à la crise : bonnes pratiques.

Se préparer à la crise:



- Connaitre et maîtriser son SI
- Socle de capacités opérationnelles
- Stratégie de communication
- Préparer sa capacité de réponses
- **S'entraîner pour s'améliorer**

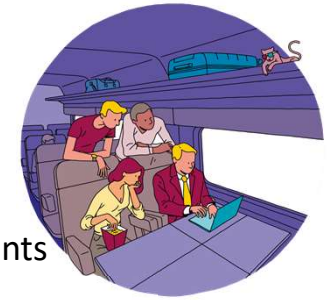
Réagir efficacement à la crise

- **Alerter, mobiliser et endiguer**
- Activer/piloter son dispositif de crise
- Activer les réseaux de soutien
- Conduire l'investigation numérique
- Mise en place des modes dégradés
- Durcissement et remédiation des SI touchés

Et moi dans tout ça ?

Je suis prudent lors de l'ouverture de pièces jointe, ou quand je clique sur un lien

Je suis vigilant lors de mes déplacements (train, hôtel, gare, etc.)



Je sépare les usages et je ne branche pas de terminaux inconnus sur mon PC professionnel

L'humain : vulnérabilité n°1

- Une bonne maturité cyber chez certains établissements, **pas de fatalité**

- Lancement du **programme CaRE** par le ministère de la santé, mobilisant tous les acteurs nationaux et locaux

- Changement d'échelle dans la réglementation cyber avec la directive **NIS 2**

Illustration : https://commons.wikimedia.org/wiki/File:We_Can_Do_It!_NARA_535413_-_Restoration_2.jpg (domaine public)

Panorama de la cybermenace 2022

Grands évènements sportifs Évaluation de la menace 2023

Rapports, alertes, IoC, recommandations :

https://www.cert.ssi.gouv.fr

et suivez les publications de l'ANSSI !

MOOC de l’ANSSI

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

SecNum*académie*.gouv.fr
Formez-vous à la sécurité du numérique

Bienvenue sur le MOOC de l'ANSSI.

Vous y trouverez l'ensemble des informations pour vous **initier à la cybersécurité**, approfondir vos connaissances, et ainsi **agir efficacement sur la protection de vos outils numériques**. Ce dispositif est accessible gratuitement. Le suivi intégral de ce dispositif vous fera bénéficier d'une attestation de réussite.

Accéder au MOOC de l'ANSSI