Webinar
IA & Cybersecurity

Sébastien Canard

September 2nd, 2024

Qu’est-ce que l’Intelligence Artificielle (IA) ?

- Larousse : « Ensemble de théories et de techniques mises en œuvre en vue de réaliser des machines capables de simuler l'intelligence humaine »
- L'IA repose sur des algorithmes, des règles et des modèles mathématiques qui traitent les données pour prendre des décisions

Algorithmes d’IA

- Différents algorithmes d’IA

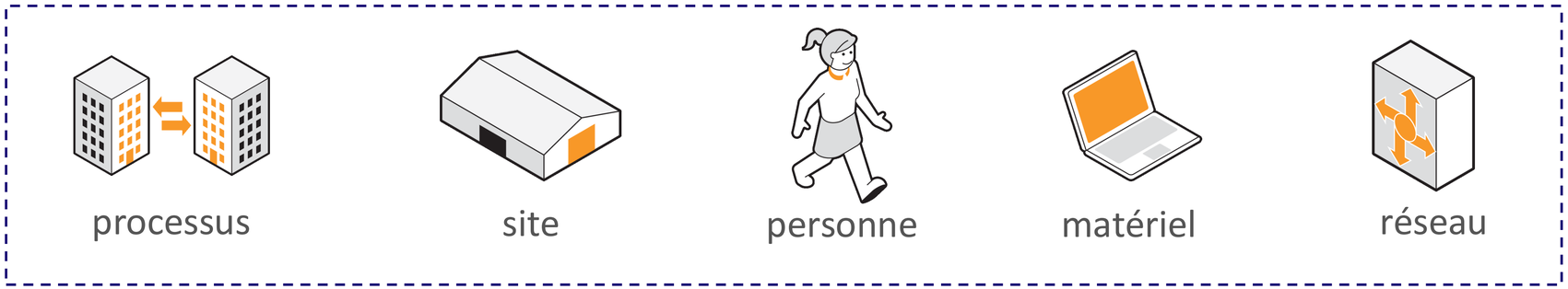
	Complexité	Type de données	Quantité de données	Exemples
Apprentissage machine	+ simple	Structurées	Faible	Régression, arbres de décision, réseaux bayésiens, forêts aléatoires, etc.
Apprentissage profond	– simple	Non-structurées	Importante	Réseaux de neurone

- De multiples applications…

Qu’est-ce que la cybersécurité ?

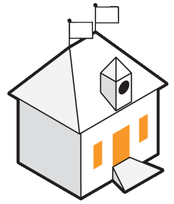
Objectif de la cybersécurité = assurer la sécurité de l’ensemble des biens d’un SI

- Système d’Informations (SI) : ensemble des ressources destinées à collecter, classifier, stocker, gérer et diffuser les informations au sein d’une organisation



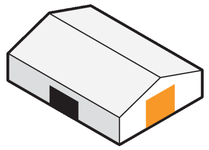
Qu’est-ce qu’une cyberattaque ?

Quelles cibles ?



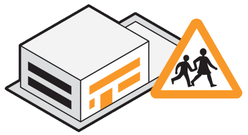
Collectivité territoriale

TPE/PME/ETI



Entreprise stratégique

Etablissement de santé



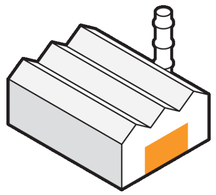
Etablissement d’enseignement supérieur

…

Quels attaquants ?

Groupe motivé par l’appât du gain

Groupe motivé par les enjeux politiques, religieux



Concurrent industriel

Etat ennemi

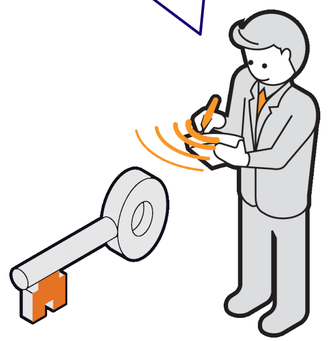
Quels impacts ?

- Financier
- Image et réputation
- Organisationnel
- Juridique et réglementaire

Quelques exemples de cyberattaques

- Prise de contrôle de machines
- Fraude interne : détournement d'avoirs, créations de fausses opérations, …
- Ingénierie sociale
- Utilisation de mots de passe faibles
- Déni de service distribué
- Phishing
- Virus
- Réseau de botnets
- Ransomware

Tout le travail d'un expert sécurité consiste à prévenir l'ensemble des cyberattaques contre le SI, ou au moins d'être capable de les maitriser.



IA & Cybersécurité :
Divorce, mariage ou cohabitation ?

IA pour les cyberattaques !

Phishing

- Utilisation de l'IA générative
- Création de messages plus convaincants, uniques
- Usurpation visuelle et sonore…

Génération de code

- Automatisation de tâches
- Génération de scripts de base, manipulation de fichiers
- Création de faux sites
- Ciblage et adaptation dynamique de malware

Ingénierie sociale

- Recherche d'informations sur les cibles
- Traductions, communications plus naturelles, etc.

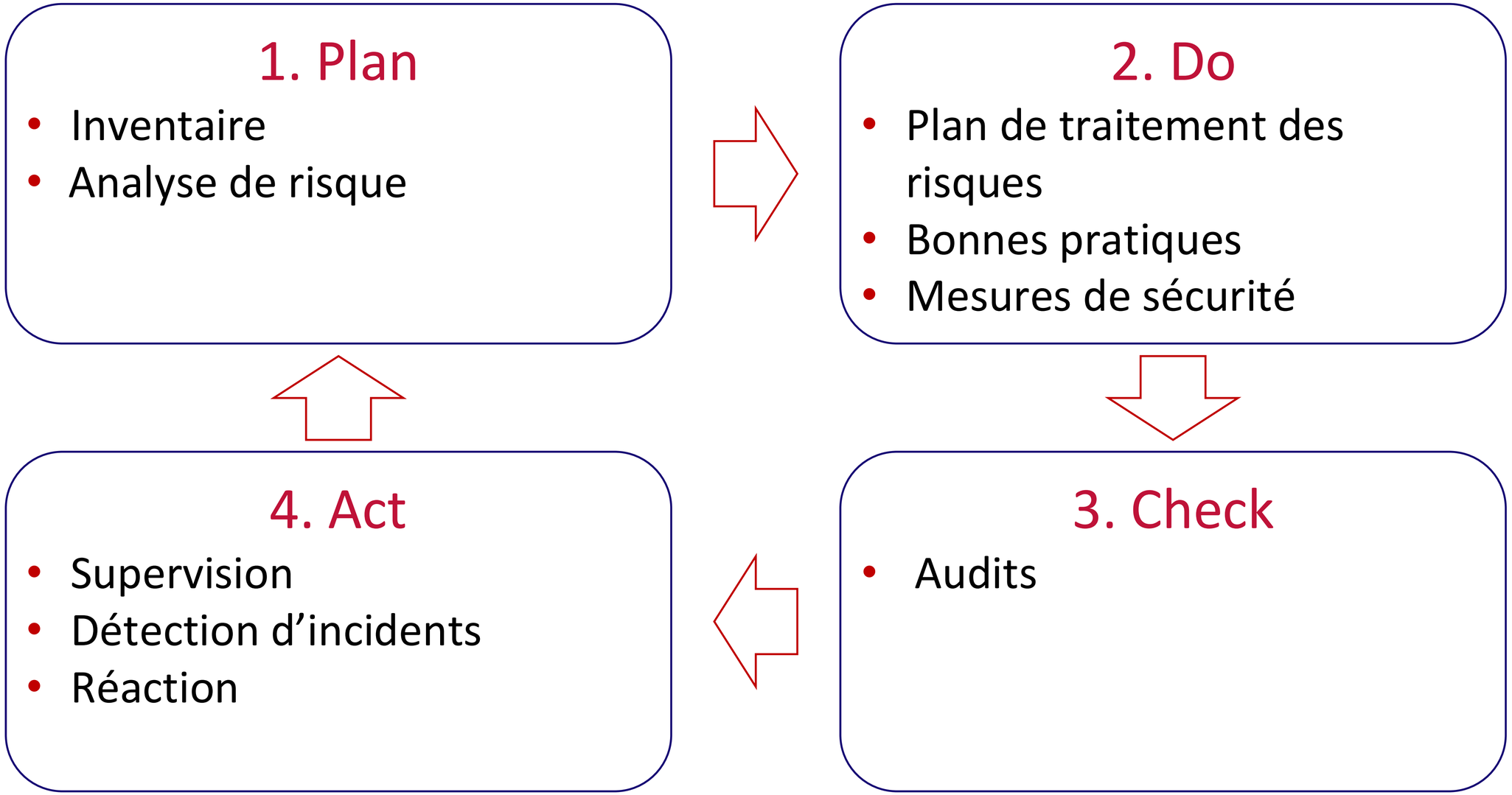
Injection de fausses informations

- Tromper les algorithmes d'IA
- Pollution des données

Meilleure compréhension des cibles

- Quelles valeurs ?
- Quelles mesures de sécurité ?
- Quels protocoles de communication ?
- Adaptation au comportement des cibles

Management de la Sécurité de l'Information

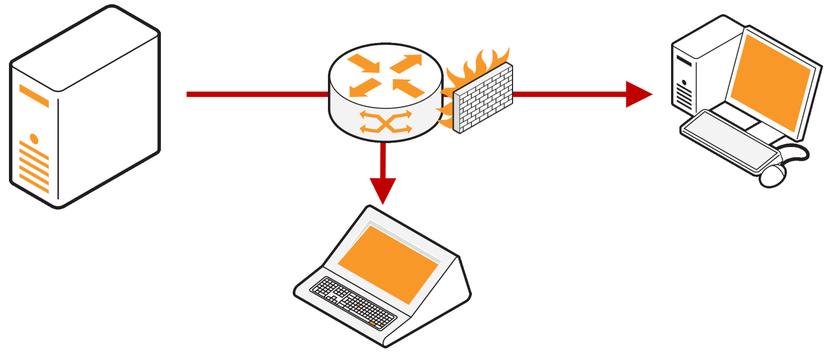


IA pour les mesures de sécurité

2. Do

Pare-feu

Intrusion Detection System (IDS)



- (Détection par signature)
- Apprentissage d'un comportement normal (LLM) ⇒ Cyberattaque si déviation
- Limitation de débits, filtrage
- Détection et utilisation de vulnérabilités de façon plus exhaustive

IA pour la supervision de la sécurité

4. Act

Centre des Opérations de Sécurité (SOC)

Surveillance des menaces et qualification des incidents



Analystes Experts Managers

SIEM/EDR/NDR

(Security Information Management System, Endpoint/Network Detection Response)

- Surveille les terminaux (ordinateurs, serveurs, téléphones, …)
- Surveille le réseau (infrastructures physiques, virtuelles et dans le cloud)
- Alertes et conformités

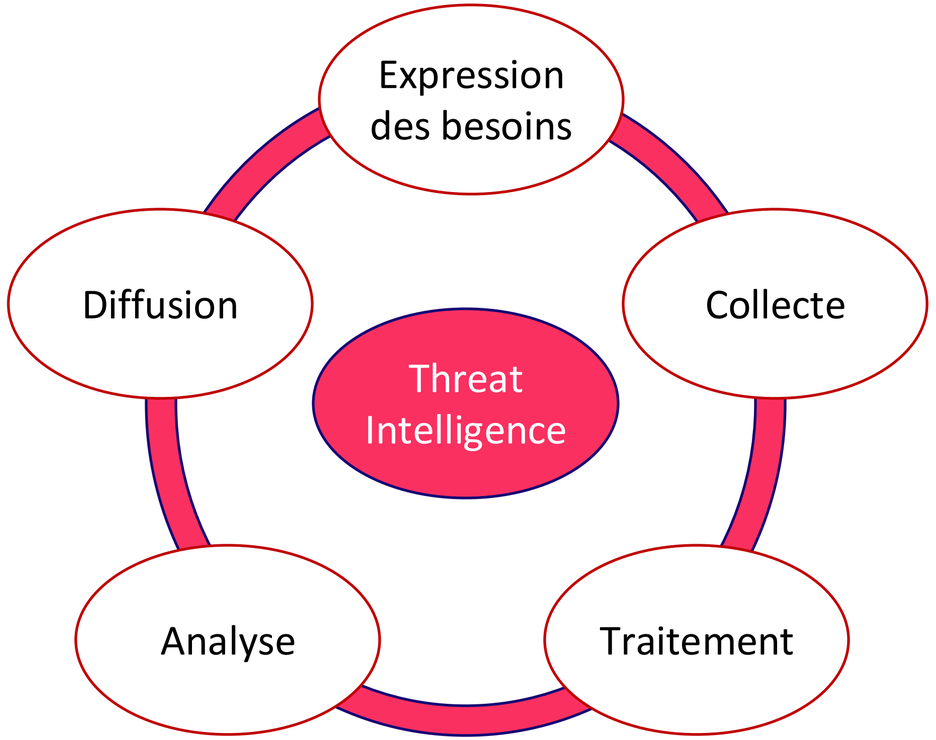
- Apprentissage d'un comportement normal et détection
- Exploitation de puits de données pour rechercher des traces d'attaques
- Plates-formes de réponse aux incidents proposant des scénarios de réaction

IA pour le renseignement

4. Act

Threat Intelligence

- Analyse poussée pour détecter les menaces présentes et futures
- Mesure de remédiation sur le long terme
- Permet d’améliorer les outils de sécurité

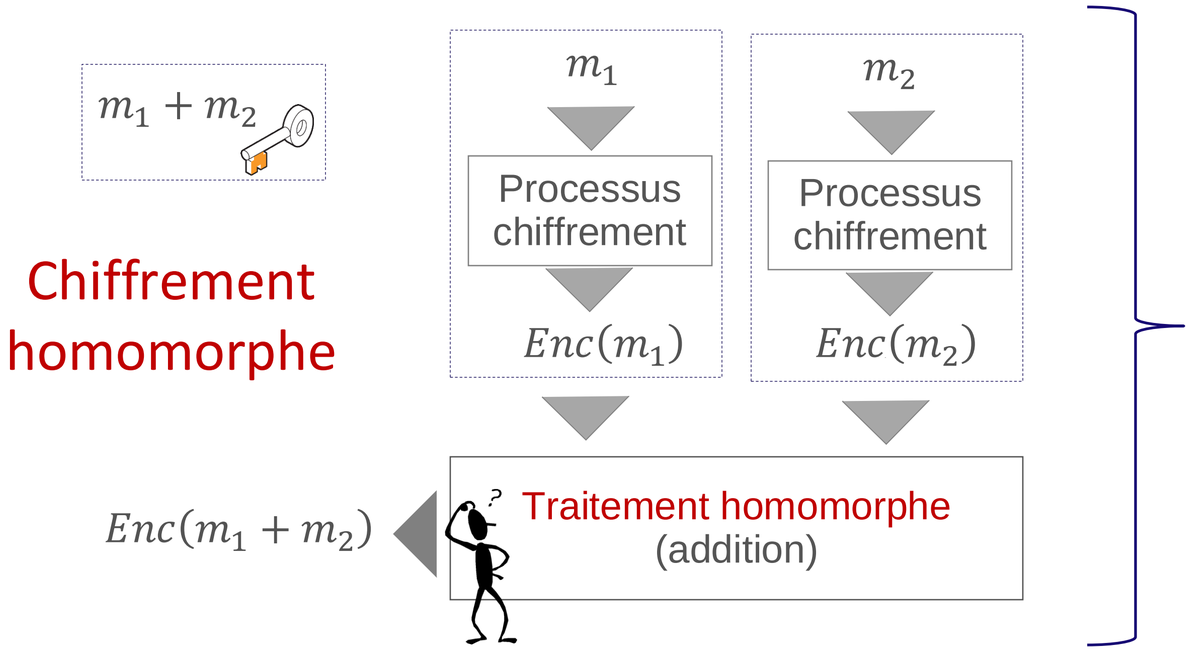


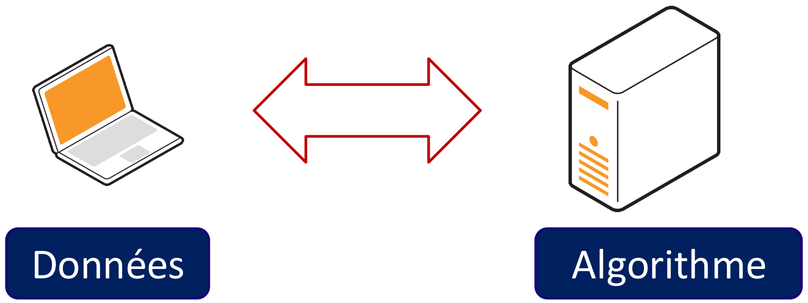
- Utilisation de multiples sources
- Parfois de façon collaborative en mode Federated Learning…

Cybersécurité pour l'IA

- Défi lié à l'IA : protection des données utilisées par les algorithmes

Utilisation de techniques de cryptographie avancée





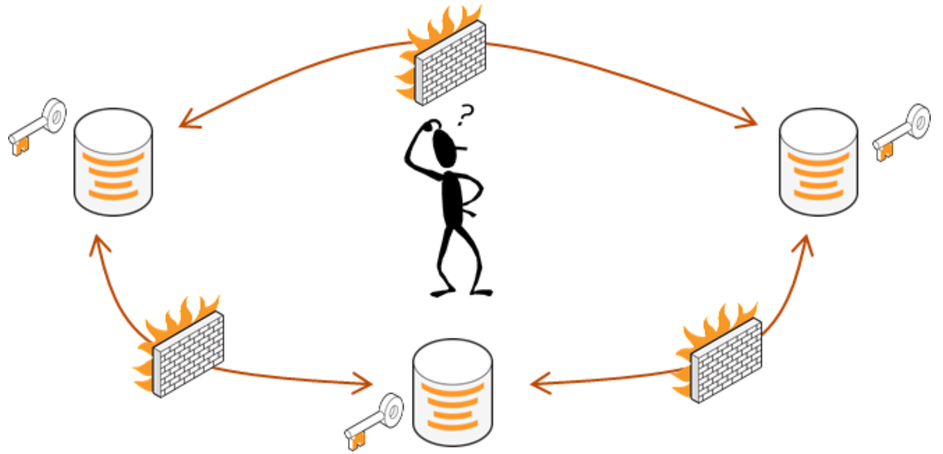
- Les données restent secrètes
- L'algorithme d'IA reste secret
- Tout ce qui transite est chiffré

Cybersécurité pour l'IA

- Défi lié à l'IA : protection des données utilisées par les algorithmes

Utilisation de techniques de cryptographie avancée

- Chaque partie garde secrète ses propres données
- Utilisation pour le Federated Learning…



Calcul multi-parties

Conclusion

- L’IA n’est qu’un outil supplémentaire utilisé par les cyberattaquants et les cyberdéfenseurs pour parvenir à leurs fins
- Mais c’est un outil extrêmement puissant
- L’exploitation des technologies d’IA n’a certainement pas encore montré ses pleines capacités

Merci