S0 : Informations générales
S1 : La donnée et la cybersécurité au cœur de nos vies
S2 : La cybersécurité pour le citoyen : la Data Privacy comme levier d'engagement
S3 : règles juridiques de la cybesécurité
S4 : Introduction à la cybersécurité logicielle
S5 : Attaques et défenses en intelligence artificielle
Introduction
Introduction à l'intelligence artificielle
Mécanismes de l'IA et réseaux de neurones
Lien entre IA et cybersécurité
Attaques et défenses
Quiz semaine 5
Evaluation finale Echéance le juil 09, 2023 at 22:00 UTC

1) QUESTION À CHOIX UNIQUE (1/1 point)

D'un point de vue pratique, l'intelligence artificielle désigne à l'heure actuelle un ensemble d'outils visant à :

○ Reproduire une intelligence humaine
● Automatiser par une machine des tâches compliquées pour un humain ✓
○ Analyser par une machine le comportement humain

AFFICHER LA RÉPONSE *Vous avez utilisé 1 essais sur 1*

2) QUESTION À CHOIX UNIQUE (1/1 point)

Le machine learning est une sous-branche :

● De l'intelligence artificielle ✓
○ De la sécurité des logiciels
○ Du calcul haute-performance

AFFICHER LA RÉPONSE *Vous avez utilisé 1 essais sur 1*

3) QUESTION À CHOIX UNIQUE (1/1 point)

L'essor actuel du machine learning est dû à :

● L'augmentation des capacités de calcul et des progrès théoriques ✓
○ L'amélioration des pratiques en architecture logicielle
○ La multiplication des objets connectés dans notre environnement

AFFICHER LA RÉPONSE *Vous avez utilisé 1 essais sur 1*

4) QUESTION À CHOIX UNIQUE (1/1 point)

Les réseaux de neurones sont une sous-branche du machine learning ?

● Vrai ✓
○ Faux

AFFICHER LA RÉPONSE *Vous avez utilisé 1 essais sur 1*

5) QUESTION À CHOIX UNIQUE (1 point possible)

Les réseaux de neurones permettent de :

○ Représenter une fonction complexe comme une composition de plusieurs fonctions très simples
○ Représenter une fonction comme la parallélisation de plusieurs fonctions très simples
● Représenter une fonction simple par la composition de fonctions complexes ✖

AFFICHER LA RÉPONSE *Vous avez utilisé 1 essais sur 1*

6) QUESTION À CHOIX UNIQUE (1/1 point)

Les réseaux de neurones s'entrainent par :

○ Essai/erreur, en modifiant aléatoirement les paramètres
● Essai/erreur, en modifiant les paramètres pour réduire un signal d'erreur ✓
○ Pas besoin, ils sont efficaces par construction

AFFICHER LA RÉPONSE *Vous avez utilisé 1 essais sur 1*

7) QUESTION À CHOIX UNIQUE (1/1 point)

L'intelligence artificielle peut servir uniquement qu'à l'attaque de systèmes cyberphysiques ?

○ Vrai
● Faux ✓

AFFICHER LA RÉPONSE *Vous avez utilisé 1 essais sur 1*

8) QUESTION À CHOIX UNIQUE (1/1 point)

L'intelligence artificielle peut être mise en défaut par un acteur malveillant :

● Vrai ✓
○ Faux

AFFICHER LA RÉPONSE *Vous avez utilisé 1 essais sur 1*

9) QUESTION À CHOIX UNIQUE (1/1 point)

Dans un cadre classique, les données utilisées pour l'entrainement d'un modèle et pour son test sont en général issues de la même distribution :

● Vrai ✓
○ Faux

AFFICHER LA RÉPONSE *Vous avez utilisé 1 essais sur 1*

10) QUESTION À CHOIX UNIQUE (1/1 point)

Il est possible de retrouver des informations sur les données de la base d'entrainement en :

○ Utilisant le concept de confidentialité différentielle
● Examinant les sorties du modèle lorsqu'on sait que la base d'entrainement a été modifiée ✓
○ Regardant l'évolution des poids du modèle quand on fait varier une entrée

AFFICHER LA RÉPONSE *Vous avez utilisé 1 essais sur 1*

11) QUESTION À CHOIX UNIQUE (1 point possible)

Il est possible d'apprendre un modèle qui se comporte comme un modèle « boite noire ».

○ Vrai dans une certaine mesure, si on peut lui soumettre un nombre important de requêtes
○ Faux, c'est impossible
● Vrai, si on connait exactement la base de données ayant servie pour l'apprentissage ✖

AFFICHER LA RÉPONSE *Vous avez utilisé 1 essais sur 1*

12) QUESTION À CHOIX UNIQUE (1/1 point)

Les exemples adversaires sont :

○ Une modification d'une donnée ayant servie à l'entrainement trompant le classifieur
● Une modification de n'importe quelle donnée trompant le classifieur ✓

AFFICHER LA RÉPONSE *Vous avez utilisé 1 essais sur 1*

13) QUESTION À CHOIX UNIQUE (1/1 point)

Un exemple adversaire pour un modèle l'est aussi pour un autre.

○ Tout le temps vrai
● Vrai assez souvent ✓
○ Vrai rarement
○ Tout le temps faux

AFFICHER LA RÉPONSE *Vous avez utilisé 1 essais sur 1*

14) QUESTION À CHOIX UNIQUE (1/1 point)

Une protection contre les exemples adversaires consiste à :

● Rajouter dans la base d'apprentissage des exemples adversaires ✓
○ Entrainer avec plus de données
○ Stopper l'entrainement avant convergence

AFFICHER LA RÉPONSE *Vous avez utilisé 1 essais sur 1*

15) QUESTION À CHOIX UNIQUE (1/1 point)

On peut créer des exemples adversaires pour un modèle « boite noire ».

○ Faux
● Vrai ✓

AFFICHER LA RÉPONSE *Vous avez utilisé 1 essais sur 1*

16) QUESTION À CHOIX UNIQUE (1/1 point)

L'attaque par empoisonnement consiste à :

○ Modifier les paramètres du modèle
○ Modifier l'exemple soumis au test
● Modifier la base d'entrainement ✓

AFFICHER LA RÉPONSE *Vous avez utilisé 1 essais sur 1*

17) QUESTION À CHOIX UNIQUE (1/1 point)

Il est possible d'insérer une marque dans un modèle (watermarking) :

○ En modifiant les poids du modèle
○ En modifiant l'architecture du modèle
● En ajoutant des exemples particuliers à la base d'apprentissage ✓

AFFICHER LA RÉPONSE *Vous avez utilisé 1 essais sur 1*

18) QUESTION À CHOIX UNIQUE (1 point possible)

Le watermarking de modèle :

● Peut détériorer les performances du modèle ✖
○ Devrait laisser inchangées ses performances

AFFICHER LA RÉPONSE *Vous avez utilisé 1 essais sur 1*

19) QUESTION À CHOIX UNIQUE (1 point possible)

On peut effacer une watermark d'un modèle.

● Si l'on connait son architecture ✖
○ Si l'on connait la base d'entrainement
○ Si l'on connait l'algorithme et la marque ayant servi à marquer le modèle

Incorrect: timely feedback -- explain why an almost correct answer is wrong

AFFICHER LA RÉPONSE *Vous avez utilisé 1 essais sur 1*

20) QUESTION À CHOIX UNIQUE (1/1 point)

La cybersécurité des algorithmes d'intelligence artificielle est :

○ Un sujet connu pour lequel des solutions existent ; seule compte la sensibilisation des utilisateurs
○ Un sujet connu pour lequel des solutions existent mais aussi des failles qu'on ne sait pas protéger
● Un sujet encore méconnu et en plein développement ✓

AFFICHER LA RÉPONSE *Vous avez utilisé 1 essais sur 1*