** Cette fiche à été générée sur DNDA Formation le 18/05/2022 à 15:05 **

Ref : DNDAFP19 | **Durée :** 3 jours | **Tarif :** 1 500 € HT

Deep learning pour Cyber security

Contenu

Objectifs :

Comprendre les défis de la cyber sécurité
Comprendre la contribution de l'IA à la prévention et à la détection des menaces
Comprendre comment l'IA peut être utilisée par les pirates
Sélectionnez des modèles d'apprentissage profond appropiate pour chaque zone de cybersécurité

Outils à maîtriser :

Tshark / Wirerequin
Tensorflow (tensorflow)
Dur
Git
Python 3 Python 3 Python 3 Python
Repères CTU-13

Module 1 : Introduction

L'ère des données
Cyber- menacesàla sécurité
Méthodologies KDD et CRISP-DM
Importance de la préparation des données

Module 2: Artificial intelligence, Machine learning & deep learning

Intelligence artificielle et machine learning
Apprentissage supervisé vs apprentissagenon supervisé
Réseaux neuronaux artificiels (ANN) et apprentissage deep (DL)
Application I: modèle prédictif basé sur lemodèle o nML
Application II: modèle prédictif basé sur ANN
Évaluation des modèles
Modèles d'apprentissage profond
Transfert d'apprentissage

Module 3 : Défis en matière de cybersécurité

Introduction
Trafic crypté Défis récents
Malware proliferation
Logiciels de sécurité/ mises à jour du firmware

Module 4: IDS / IPS en utilisant l'apprentissage deep

Introduction
IDS vs pare-feu
IDS vs IPS
Modèles de penchement de machine pour la détection d'intrusion
Modèles d'apprentissage profond pour la détection intrusion
L'apprentissage par ensemble comme alternative aux modèles d'apprentissage profond

Module 5 : Applications d'apprentissage profond fou cybersécurité

Renseignements sur les menaces
Vidéosurveillance intelligente : IVS
Détection des anomalies

LAB : Atténuation de la DGA

Problème de la DGA
Ensembles de données 1M
Signatures de construction
Prétraitement des données
Conception du modèle
Formation du modèle
Tester le modèle
Comment déployer le model?
Comment mettre à jour le modèle.

Module 6 : Application d'apprentissage profondpour trafic crypté

TLS et https
Poignée de main TLS
Approches basées sur les fonctionnalités
Approches métriques
Approches basées sur le flux
Classification de la circulation et empreintes digitales

Module 7 : Modèles accusatoires génératifs: GANs

Introduction
Composants d'apprentissage profond GAN
GAN avantages
Comment les GANs peuvent-ils être used pour générer des attaques?
Comment atténuer généré unttacks? L'apprentissage profond à la rescousse!

Module 8 : Comment intégrer un modèle d’apprentissage profond dans une pile de cybersecurity?

ETL et pipelines de données
Siem
API comme emballage
Heuristics et notation approdouleurs

Public

SOC. Analystes, Experts en sécurité, Experts en intelligence de menace et Experts en gestion des risques.

Pré-requis

Comprendre les bases de routage et de switching du réseau, savoir-faire de base des boucliers de protection et comprendre les bases des algorithmes de cryptage et du chiffrement-suites.

Méthodes pédagogiques

Alternance d'apports théoriques, d'exercices pratiques et d'études de cas.