Opleiding : Kunstmatige intelligentie en operationele beveiliging

AI als een gebied van mogelijkheden voor kwaadwillige handelingen

Synthese cursus - 1d - 7u00 - Ref. ICY

Prijs : 850 € V.B.

4,1 / 5

Deze cursus helpt je te begrijpen wat kunstmatige intelligentie (AI) is, hoe je het kunt definiëren in de context van cyberbeveiliging, het belang van het beveiligen van onze verbonden objecten, onze identiteiten, onze persoonlijke gegevens, enz. en het belang van operationele beveiliging.

Pedagogische doelstellingen

Aan het einde van de training is de deelnemer in staat om:

- Begrijpen hoe kunstmatige intelligentie nuttig kan zijn voor cyberbeveiliging
- De beveiligingsproblemen van verbonden objecten begrijpen
- Ontdek de tools en hulpmiddelen voor het detecteren van social engineering, biometrische en spoofingaanvallen...

Doelgroep

Beslissers, projectmanagers, ingenieurs, ontwikkelaars, onderzoekers.

Voorafgaande vereisten

Voorkennis van een computertaal en een programmeertaal.

Opleidingsprogramma

DEELNEMERS

Beslissers, projectmanagers, ingenieurs, ontwikkelaars, onderzoekers.

VOORAFGAANDE VEREISTEN

Voorkennis van een computertaal en een programmeertaal.

VAARDIGHEDEN VAN DE CURSUSLEIDER

De deskundigen die de cursus leiden zijn specialisten op het betreffende vakgebied. Zij werden geselecteerd door onze pedagogische teams zowel om hun vakkennis als hun pedagogische vaardigheden voor elke cursus die zij geven. Zij hebben minstens vijf tot tien jaar ervaring in hun vakgebied en oefenen of oefenden verantwoordelijke bedrijfsfuncties uit.

BEOORDELINGSMODALITEITEN

De cursusleider beoordeelt de pedagogische vooruitgang van de deelnemer gedurende de gehele cursus aan de hand van meerkeuzevragen, praktijksituaties, praktische opdrachten, ...
De deelnemer legt ook van tevoren en naderhand een test af ter bevestiging van de verworven kennis.

1 De uitdagingen tussen AI, robotica en cyberbeveiliging definiëren

- Definitie en concepten.
- De inzet voor overheden, legers en alle IT-gerelateerde organisaties.
- De mogelijkheden en grenzen van AI-gerelateerde cyberbeveiliging.
- Softwarebedreigingen. Malwaredetectietools.
- Beveiligingsproblemen met betrekking tot het internet der dingen (IoT).
- Mogelijkheden en grenzen van het internet van de dingen in een context van cyberbeveiliging.
- Kwaadaardige verbonden objecten versus detectiemiddelen.

Demonstratie

Demonstraties: polymorfe software, genetische algoritmen voor het genereren van polymorfe code, elektronische en robotische hardware.

2 Social engineering en kunstmatige intelligentie

- Wat is een social engineering-aanval? Wat zijn de gevolgen?
- Principes van "deepfakes" (valse identiteiten, afbeeldingen, stemmen en video's).
- Mogelijkheden en grenzen van een GAN (Generative Adversarial Networks).
- Nieuwe detectietools

Demonstratie

Implementatie van een GAN-netwerk om afbeeldingen met dummy stijlen te produceren.

3 AI als hulpmiddel voor detectie, bescherming, bewaking, identificatie...

- Systemen van steeds toenemende "complexiteit".
- Statistische indicatoren "klassiek" onvoldoende om een complex systeem te bewaken.
- Machine learning (ML) en deep learning (DP) voor het opsporen en voorkomen van anomalieën.
- AI als bewakingsinstrument. Gebruik van ML en DL door biometrische systemen.
- Mogelijkheden en grenzen van ML en DL bij de identificatie van individuen.
- Misbruik: fout-positieven, fout-negatieven, kwaadwillige handelingen, enz.

Demonstratie

Detectiemodel. Typologie van camera's (360, HD, 3D-RGBd...).
Demonstraties van de beperkingen, "vooroordelen" die samenhangen met AI en gevallen waarin AI effectiever is dan het menselijk oog.

4 AI-gestuurd luisteren

- Afluistercontext "versterkt" met kunstmatige intelligentie.
- Tools en hulpmiddelen voor het afluisteren van een gesprek, het opsporen van een geheime code, het reconstrueren van een e-mail, enz.
- Succesvolle projecten toegankelijk voor iedereen.
- Hoe kunnen we de vertrouwelijkheid van onze uitwisselingen garanderen?
- Mogelijkheden en grenzen tussen "frappologie" en AI. Hoe kunnen we onszelf beschermen?

Demonstratie

Hulpmiddelen en onderzoek voor het reconstrueren en voorspellen van indirecte signalen in een lawaaiige omgeving.

PEDAGOGISCHE EN TECHNISCHE MIDDELEN

• De gebruikte pedagogische middelen en cursusmethoden zijn voornamelijk: audiovisuele hulpmiddelen, documentatie en cursusmateriaal, praktische oefeningen en correcties van de oefeningen voor praktijkstages, casestudies of reële voorbeelden voor de seminars.
• Na afloop van de stages of seminars verstrekt ORSYS de deelnemers een evaluatievragenlijst over de cursus die vervolgens door onze pedagogische teams wordt geanalyseerd.
• Na afloop van de cursus wordt een presentielijst per halve dag verstrekt, evenals een verklaring van de afronding van de cursus indien de stagiair alle sessies heeft bijgewoond.

TOEGANGSMODALITEITEN EN TERMIJNEN

De inschrijving dient 24 uur voor aanvang van de cursus plaatsgevonden te hebben.

TOEGANKELIJKHEID VOOR MINDERVALIDEN

Is voor u speciale toegankelijkheid vereist? Neem contact op met mevr. FOSSE, contactpersoon voor mindervaliden, via het adres psh-accueil@ORSYS.fr om uw verzoek en de haalbaarheid daarvan zo goed mogelijk te bestuderen.