ARTIFICIAL INTELLIGENCE USAGE in CYBER SECURITY

Definition of training:
It is known that artificial intelligence and machine learning provide some important advantages for modern cyber security applications over traditional applications. The power of machine learning applications to present findings on experiential learning and how to strategize when faced with similar problems in the future can be considered as an advantage compared to traditional passive applications. Machine learning has a role to play in helping organizations improve their capabilities across all five security categories—prediction, prevention, detection, response and monitoring. Machine learning can learn from existing data to make decisions when faced with new data in areas such as network traffic analysis, fraud detection and user behavior. This enables it to detect different types of attacks across layers of security, from network to application, endpoint and user level. Our training titled "Artificial Intelligence in Cyber Security" aims to teach institutions how and where artificial intelligence and machine learning methods can be used in the field of cyber security. It is aimed to reorganize the data with preprocessing, to obtain prediction and classification models by applying machine learning algorithms, then to apply the testing and evaluation processes of these models on real data sets and to create awareness. In the training, algorithms such as Recurrent Neural Networks (RNN), LSTM and Autoencoders based on Tensor flow Keras libraries will be applied on datasets, with a particular focus on deep learning algorithms.

Duration:
2 Days (12 Hours)

Place:
A classroom with an internet connection that can accommodate up to 20 attendees.

Target group:
Institutions considering using artificial intelligence technologies in cyber security and people interested in the subject.

Participation prerequisite:
Participants need to know R or Python programming language.

Document:
Certificate of participation

AIUCS_ENG.11/2022_V1