Siber Güvenlikte Yapay Zekâ

Eğitimin tanımı:

Yapay zekâ ve makine öğrenmesinin modern siber güvenlik uygulamaları için geleneksel uygulamalara göre bazı önemli avantajlar sağladığı bilinmektedir. Makine öğrenmesi uygulamalarının deneyime dayalı öğrenme ve gelecekteki benzer sorunlarla karşılaşıldığında nasıl bir strateji izleneceğine ilişkin bulguları sunma gücü, geleneksel pasif uygulamalara kıyasla bir avantaj olarak değerlendirilebilir. Makine öğrenmesi tahmin, önleme, tespit, yanıt ve izleme gibi beş güvenlik kategorisinin tamamında kuruluşların yeteneklerini geliştirmeye yardımcı olmada rol oynaması söz konusudur.

Makine öğrenmesi, ağ trafiği analizi, sahtekarlık tespiti ve kullanıcı davranışı gibi alanlarda yeni verilerle karşılaştığında karar vermeyi var olan verilerden öğrenebilir. Bu, ağdan uygulamaya, uç noktaya ve kullanıcı seviyesine kadar güvenlik katmanları arasında farklı tipte saldırıları tespit etmesini sağlar.

"Siber Güvenlikte Yapay Zeka" başlıklı eğitimimiz, kurumlara yapay zekâ ve makine öğrenmesi yöntemlerinin siber güvenlik alanında nasıl ve nerelerde kullanılabileceğini öğretmeye yöneliktir. Ön işleme ile verinin yeniden düzenlenmesi, makine öğrenmesi algoritmalarının uygulanarak tahmin ve sınıflama modellerinin elde edilmesi ardından bu modellerin test ve değerlendirme süreçlerini gerçek veri kümeleri üzerinde uygulanması ve farkındalığın yaratılması amaçlanmaktadır. Eğitimde özellikle ***derin öğrenme*** algoritmalarına odaklanarak, veri kümeleri üzerinde Tensorflow Keras kütüphanelerine dayalı *Geri Dönüşlü Derin Öğrenme (Recurrent Neural Networks =RNN), LSTM* ve *Otomatik Kodlayıcılar (Autoencoders)* gibi algoritmalar uygulanacaktır.

Süre:

2 gün (toplam 12 saat)

Yer:

En fazla 20 öğrencinin katılabileceği, internet bağlantısı olan bir sınıf.

Hedef Kitle:

Siber güvenlikte yapay zekâ teknolojilerini kullanmayı düşünen kurumlar ve konuyla ilgilenen kişiler.

Katılım Ön Şartı:

R veya Python programlama diline aşina olmak.

Belge:

Katılım belgesi.