CAP450 : Security in Artificial Intelligence

The Security in Artificial Intelligence course examines the principles of information and software development security, AI-based tools used to identify and respond to threats, and endeavors developed to work against AI algorithms. This course explores how to secure AI algorithms against malicious use, including methods used to exploit AI weaknesses and how machine learning can be leveraged by adversaries. Students will investigate security architecture, engineering and operations, and use of AI-based tools.
Credits 3