- Filename: eccouncil-ceh31250-v11-1-17-1-ml-and-ai.md
- Show Name: CEHv11 (312-50)
- Topic Name: Intro to Ethical Hacking
- Episode Name: ML and AI

==========

ML and AI

Objectives:

- Examine the role of AI and ML in Cybersecurity
- Identify AI/ML classifications
- Define the 9 main Cybersecurity areas/categories that utilize AI/ML
- Determine how AI/ML aid in the prevention of cyber attacks

- What is Artificial Intelligence?
    - Computers that are built to mimic human behavior
        - Specifically...
            - Problem Solving
            - Decision Making
- What is Machine Learning?
    - Subset of AI
    - Gives the AI the ability to LEARN
        - **Learning Techniques**
            1. *Supervised Learning*
        - ML is provided with Labeled Datasets
            - These train the ML to classify data and/or to predict outcomes
        - 2 Problem Types (what problems does this solve?)
            - `Classification`
                - Classify or categorize data into defined groups
                    - Apples and Oranges
                    - Spam or Valid Email
            - `Regression`
                - Discerns the relationship between independent and dependent variables
                - Good at predicting numerical values
                    - Sales revenue projections
            2. *Un-supervised Learning*
        - Analyze and cluster UNLABLED DATA SETS
            - Discovers hidden patterns without help from humans
        - 3 Problem Types
            - `Clustering`
                - Grouping unlabeled data based on similarities/differences

        - `Association`
            - Discovers relationships between variables in given dataset
                - Customers who bought this also bought x
        - `Dimensionality Reduction`
            - Reduces high number of data inputs to a manageable size
                - Reduction doesn't affect data integrity
                    - Picture quality improvement algorithms
- How is ML and AI being used in the Cybersecurity space?
    - Endpoint Security
    - Authentication
    - Phishing
    - Threat Detection
    - Vulnerability Assessment and Management
    - Behavioral Analysis
    - Network Security
    - AI vs AI