Cybersecurity Data Science

Modality: On Demand

Duration: 1 Hour

About this Course:

The best of the best badass hackers and security experts are using machine learning to break and secure systems. This course has everything you need to join their ranks.

In this one-of-its-kind course, we will be covering all from the fundamentals of cybersecurity data science, to the state of the art. We will be setting up a cybersecurity lab, building classifiers to detect malware, training deep neural networks and even breaking CAPTCHA systems using machine learning.

If you've tried to enter the super hot field of cybersecurity and machine learning, but faced rejection after rejection, needing experience to get experience, feeling hopeless that the demand and pay are so high, but nothing you are doing is letting you in, this is your chance to gain an edge over the competition. This is your chance to get credentials and real experience.

If you are looking to break into the field of cybersecurity data science, pick up on the bleeding edge tools, and *become the best in the field of cybersecurity*, this course is for you.

We will be using python and scikit learn for majority of our machine learning, and keras, a wrapper for tensorflow, for deep learning. This course is hands on and practical. Consequently, a student is expected to put in the work and not be shy about getting their hands dirty with some malware!

Course Objectives:

- Use machine learning to classify malware.
- Malware analysis 101.
- Set up a cybersecurity lab environment.
- Learn how to tackle data class imbalance.
- Unsupervised anomaly detection.
- End-to-end deep neural networks for malware classification.
- Create a machine learning Intrusion Detection System (IDS).
- Employ machine learning for offensive security.
- Learn how to address False Positive constraints.
- Break a CAPTCHA system using machine learning.

Audience:

- Data scientists curious to apply the craft to the field of cybersecurity.
- Cybersecurity experts curious to see how data science can be applied to cybersecurity.

Prerequisites:

- Basic programming in python.
- Basic knowledge of data science.

Course Outline:

- Introduction
    - Course Overview
- **Machine learning and Malware Detection**
    - Setting Up Your Lab Environment
    - Setting Up a Lab Environment - Assignment
    - Obtaining a Malware Dataset
    - Obtaining a Benign Dataset
    - Malware Analysis 101
    - Malware Analysis 101 - Assignment
    - PE File: Introduction
    - PE File - Quiz
    - Installing the Pefile Library
    - Extracting PE Information Using pefile
    - Preparing a Corpus Using pefile - Assignment
    - TF-IDF
    - Creating a Train-Test Split
    - Training a Classifier
    - Training a Classifier - Assignment
    - Tackling Class Imbalance
    - Handling Type I and Type II Errors
    - N-grams
    - N-grams - Assignment
    - Hash-Grams
    - Building an N-gram Classifier
    - MalConv: Deep Learning on Executables
- **Machine Learning and Intrusion Detection**
    - The KDD Cup Dataset
    - Isolation Forest
- **Machine Learning and Offensive Security**
    - Really Simple CAPTCHA
    - Really Simple CAPTCHA - Assignment
    - Preprocessing CAPTCHAs
    - Training a CAPTCHA Recognizer