ADVANCED AI FOR CYBERSECURITY PROFESSIONALS

Expert-Led Cybersecurity Training · Beginner to Advanced

COURSE OVERVIEW

The "Advanced AI for Cybersecurity Professionals" course is designed as an intensive learning experience for cybersecurity practitioners seeking to enhance their skills in utilizing cutting-edge AI technologies within the realm of cybersecurity. This course offers a deep dive into the intricate convergence of machine learning (ML), neural networks, large language models (LLMs), and their practical applications in strengthening cybersecurity frameworks. Participants will be equipped with the knowledge and tools necessary to proactively defend digital assets against evolving cyber threats while also gaining hands-on experience in developing AI-powered security solutions.

The curriculum begins with an exploration of foundational concepts in machine learning, distinguishing between supervised and unsupervised learning and delving into the applications of essential ML algorithms such as Linear Regression, Decision Trees, Random Forests, and Support Vector Machines (SVM). Participants will gain proficiency in utilizing K-Means Clustering and Principal Component Analysis (PCA) for data analysis, along with practical experience in implementing these algorithms using tools like Pandas, scikit-learn, and statsmodel. The course emphasizes the importance of training, testing, and validation sets in ensuring model accuracy and reliability, while also addressing strategies for reducing loss through techniques like Stochastic Gradient Descent and optimizing learning rates.

Moving further, the course covers advanced topics in anomaly detection using ML, including real-world scenarios such as credit card fraud detection and identifying network attacks through machine learning algorithms. Participants will delve into the realm of neural networks and LLMs, understanding the underlying mechanisms of these models and exploring popular open-source LLMs along with their diverse use cases. Special attention is given to security challenges inherent in LLM applications, along with techniques like Langchain agents, RAG, Fine-Tuning LLM models with Custom Data, and tools like LLamaIndex and Streamlit for effective querying of multiple data sources and building full-stack AI applications.

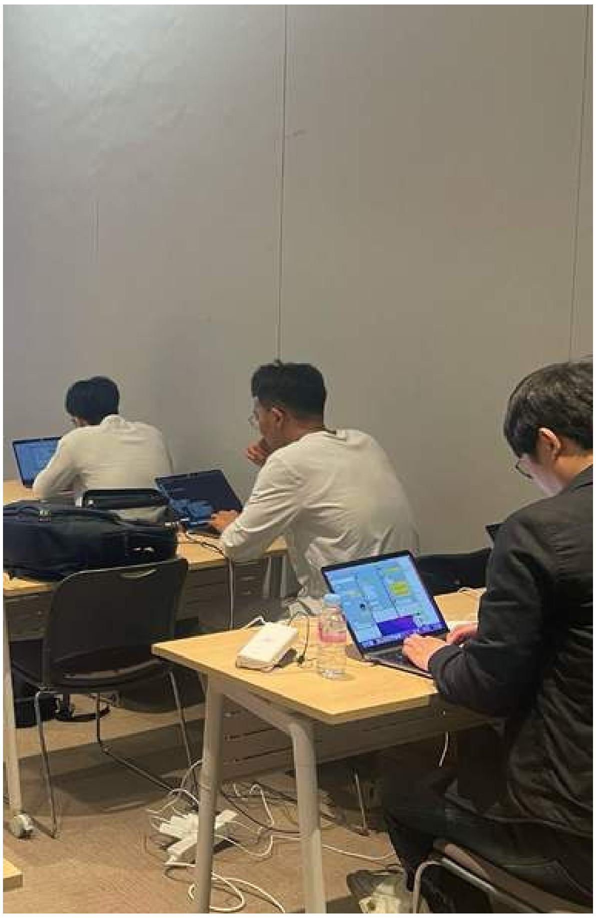
Moreover, the course addresses the complexities of working with extremely large datasets, leveraging vector indexes and databases for efficient data processing and analysis. It concludes with a forward-looking discussion on the future of AI in cybersecurity, highlighting emerging trends, challenges, and opportunities in the rapidly evolving landscape of AI-driven security solutions.

WHY SHOULD YOU TAKE THIS COURSE?

This is a completely hands-on course designed for beginners and intermediate students. Instead of just slides, attendees will get a chance to exploit all of the vulnerabilities taught by the instructors. The slack channel is created before the course for the students so that they can be adequately prepped in terms of hardware and software before the class.

KEY LEARNING OBJECTIVES

- Intro to Machine Learning – Supervised vs Unsupervised Learning
- Applications of Linear Regression, Decision Trees, Random Forests, and Support Vector Machines (SVM)
- Applications of K-Means Clustering and Principal Component Analysis (PCA)
- Introduction to Pandas, scikit-learn, and statsmodel
- Training, testing, and Validation Sets
- Reducing Loss – Stochastic Gradient Descent, Learning Rate
- Anomaly Detection using ML with labs
- Intro to Neural Networks and LLMs
- How Large Language Models work?
- Popular Open Source LLMs and their use cases
- Security Challenges in LLM applications
- Langchain agents
- RAG and Fine-Tuning LLM models with Custom Data
- LLamaIndex and Streamlit
- Querying Multiple Data sources
- Vector Indexes and Vector Databases
- Building a full-stack AI app
- Working with Extremely Large Datasets
- Conclusion and Future of AI



WHO SHOULD ATTEND?

This course is for anyone who wants to enhance their knowledge of AI and use it in the field of Cybersecurity.

PREREQUISITE KNOWLEDGE

- Working knowledge of cybersecurity and pentesting fundamentals
- Basic understanding of Artificial Intelligence and Machine Learning fundamentals
- Understanding of principles of data science and learning algorithms
- Understanding of fundamental programming concepts and looping structures in at least one higher-level language used in machine learning (eg: Python, or similar)

WHAT WILL THE STUDENT GET?

- Certificate of completion for the Training program
- Cloud Access for attendees (Live On-site & Virtual Training only)
- Huge list of good reads and articles for learning mobile security
- Source code for vulnerable applications
- Slack access for the class and after for regular mobile security discussions (Live On-site & Virtual Training only)

HARDWARE/SOFTWARE REQUIREMENT

- Laptop with 8+ GB RAM and 40 GB hard disk space
- Students will be provided with access to Linux cloud instances
- Students will be provided with access to Corellium for iOS hands-on and as such do not need to carry iOS devices
- Administrative access on the system

Detailed Course Setup instructions and Slack access will be sent a few weeks prior to the class (Live On-site & Virtual Training only)

COURSE SYLLABUS

Module 1: Introduction to Machine Learning Fundamentals

- Understanding Supervised vs Unsupervised Learning
- Exploring Linear Regression, Decision Trees, Random Forests, and Support Vector Machines (SVM)
- Applications of K-Means Clustering and Principal Component Analysis (PCA)
- Introduction to Pandas, scikit-learn, and statsmodel libraries
- Practical Training on Creating Training, Testing, and Validation Sets
- Strategies for Reducing Loss: Stochastic Gradient Descent, Learning Rate Optimization

Module 2: Advanced Machine Learning Techniques

- Anomaly Detection using Machine Learning
- Real-world Applications and Use Cases
- Lab Exercises on Anomaly Detection Techniques
- Case Study: Credit Card Fraud Detection using ML algorithms
- Case Study: Detecting Network Attacks using ML algorithms

Module 3: Leveraging AI for Building Pentest Tools

- Understanding the Role of AI in Cybersecurity and Pentesting
- AI-Powered Vulnerability Detection and Exploitation
- Building Custom Pentest Tools using ML Algorithms
- Practical Hands-on Session: Developing an AI-Based Pentest Tool

Module 4: Understanding Neural Networks and Large Language Models (LLMs)

- Basics of Neural Networks
- Understanding the Working Principles of Large Language Models
- Exploring Popular Open Source LLMs and their Use Cases
- Security Challenges in Large Language Model Applications
- Owasp Top 10 for LLMs
- Techniques like Langchain agents, RAG, and Fine-Tuning LLM models with Custom Data
- Hands-on tutorials on utilizing pre-trained LLMs for automating tasks such as reconnaissance.
- Best practices for fine-tuning LLMs for specific cyber operation tasks

Module 5: Advanced Data Handling Techniques

- Utilizing LLamaIndex for Data Management
- Using LangChain to build Custom chains
- Working with Multiple Data Sources and Integration
- Handling Extremely Large Datasets with Efficient Data Processing Techniques
- Leveraging Vector Indexes and Vector Databases for Data Analysis

Module 6: Building Full-Stack AI Applications for Cybersecurity

- Introduction to Full-Stack Development for AI Applications
- Integrating AI Security Tools into Existing Cybersecurity Frameworks
- Practical Guide to Building Full-Stack AI Apps
- Hands-on Project: Developing a Full-Stack AI App for Cybersecurity

Module 7: Conclusion, Future Trends, and Challenges

- Recap of Course Learnings and Key Takeaways
- Future Trends and Innovations in AI for Cybersecurity
- Challenges and Opportunities in the Evolving Landscape of AI-driven Security Solutions

About the company

8kSec is a foremost cyber security research company offering exceptional training and consulting services to aid clients in enhancing their security stance. Our experts possess extensive experience in delivering specialized cybersecurity training and consulting to multiple commercial and defense organizations across the United States, Europe, and the Middle East and North Africa region.

Get in touch

8kSec.io
info@8ksec.io

The information in this document is subject to change without notice.