AI and Machine Learning for Advanced Cyber Defense Training Course



19 - 23 Oct 2026

Cape town

4600 € (Per Person)

Ref: #CYB9702_272254

Course Introduction / Overview:

In an era where cyber threats are evolving with unprecedented speed and sophistication, traditional defense mechanisms are no longer sufficient. This course provides a comprehensive exploration of how Artificial Intelligence (AI) and Machine Learning (ML) are revolutionizing the cybersecurity landscape. We will delve into the core principles that enable systems to predict, detect, and respond to cyber-attacks with greater accuracy and speed than humanly possible. As discussed by author Leslie F. Sikos in his work "AI in Cybersecurity," the proactive and adaptive nature of AI is the key to defending against modern, automated threats. This program, offered by BIG BEN Training Center, is meticulously designed to bridge the gap between theoretical data science and practical cybersecurity application. Participants will move beyond buzzwords to gain hands-on experience in building and deploying ML models for tasks such as malware analysis, network intrusion detection, and automated incident response. The curriculum is structured to empower professionals with the skills to leverage AI-driven security analytics, transforming their organization's defensive posture from reactive to predictive and creating a resilient security infrastructure for the future.

Target Audience / This training course is suitable for:

- Cybersecurity Analysts and Engineers.
- Security Operations Center (SOC) Managers and Team Leads.
- Threat Intelligence Analysts.
- IT Security Professionals and Architects.
- Network Security Engineers.
- Data Scientists and Analysts with an interest in security.
- Incident Responders and Digital Forensics Investigators.
- IT Managers and Directors overseeing security functions.
- Software Developers building secure applications.
- Information Security Consultants.

Target Sectors and Industries:

- Financial Services and Banking.
- Healthcare and Medical Institutions.
- Government and Public Sector Agencies.
- Defense and Military Sectors.
- Telecommunications and Technology.
- Critical Infrastructure and Energy.
- E-commerce and Retail.
- Consulting and Professional Services.

Target Organizations Departments:

- Information Security Department.
- Cybersecurity Operations.
- Security Operations Center (SOC).
- Information Technology (IT) Department.
- Risk and Compliance Management.
- Threat Intelligence and Hunting Teams.
- Research and Development (R&D).
- Incident Response and Forensics Units.

Course Offerings:

By the end of this course, the participants will have able to:

- Develop a foundational understanding of AI and ML concepts in the context of cyber defense.
- Apply supervised learning algorithms for malware classification and spam detection.
- Utilize unsupervised learning techniques for network anomaly and intrusion detection.
- Implement deep learning models for advanced threat analysis and identification.
- Design and automate AI-driven incident response and threat hunting workflows.
- Analyze and defend against adversarial attacks targeting machine learning models.
- Evaluate the performance and effectiveness of AI-based security solutions.
- Integrate AI and ML capabilities into existing security information and event management (SIEM) systems.
- Understand the ethical considerations and biases in using AI for security.
- Formulate a strategic plan for adopting AI in their organization's cybersecurity framework.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, practical, and highly interactive, ensuring that participants not only learn the theory but can also apply it effectively. This course moves beyond traditional lectures by incorporating extensive hands-on labs where participants will work with real-world, anonymized security datasets. They will build, train, and test machine learning models using industry-standard tools and programming languages. The learning process is reinforced through detailed case studies of major cyber-attacks where AI could have played a decisive role in prevention or mitigation. Collaborative group projects and team-based problem-solving sessions encourage participants to share insights and tackle complex security challenges together. Our expert instructors facilitate dynamic discussions, providing personalized feedback and guiding participants through complex topics. The curriculum emphasizes a practical, problem-centric approach, ensuring that every concept is linked to a tangible cyber defense application. This blend of expert instruction, practical application, and collaborative learning creates a robust educational experience that equips professionals with immediately applicable skills.

Course Agenda (Course Units):

Unit One: Foundations of AI and ML in a Cybersecurity Context

- Introduction to Artificial Intelligence, Machine Learning, and Deep Learning.
- The Evolving Cyber Threat Landscape and the Limits of Traditional Defense.
- Key Mathematical and Statistical Concepts for ML in Security.
- The Role of Data Science in Cybersecurity Analytics.
- Understanding the ML Project Lifecycle for Security Applications.
- Exploring Python Libraries for Security Data Analysis (e.g., Pandas, Scikit-learn).
- Ethical Considerations and Data Privacy in AI-driven Security.

Unit Two: Supervised Learning for Threat Detection and Classification

- Understanding Classification, Regression, and Ensemble Methods.
- Implementing Logistic Regression and Support Vector Machines (SVM) for Phishing Detection.
- Building Decision Trees and Random Forests for Malware Family Classification.
- Analyzing Network Traffic for Malicious Activity using Supervised Models.
- Feature Engineering and Selection for Security Datasets.
- Model Evaluation Metrics: Accuracy, Precision, Recall, and F1-Score.
- Hands-on Lab: Training a Model to Classify Malicious vs. Benign URLs.

Unit Three: Unsupervised Learning for Anomaly and Intrusion Detection

- Core Concepts of Clustering and Dimensionality Reduction.
- Applying K-Means Clustering for Network Traffic Anomaly Detection.
- Using Density-Based Scanning (DBSCAN) to Identify Outliers in User Behavior.
- Principal Component Analysis (PCA) for Visualizing High-Dimensional Security Data.
- Building an Unsupervised Network Intrusion Detection System (NIDS).
- Techniques for Profiling Normal System and User Behavior.
- Hands-on Lab: Detecting Anomalous Logins with Unsupervised Algorithms.

Unit Four: Deep Learning for Advanced Cyber Defense

- Introduction to Neural Networks and Deep Learning Architectures.
- Using Artificial Neural Networks (ANNs) for Complex Threat Patterns.
- Applying Convolutional Neural Networks (CNNs) for Malware Image Analysis.
- Leveraging Recurrent Neural Networks (RNNs) for Analyzing Sequential Log Data.
- Introduction to Generative Adversarial Networks (GANs) for Threat Modeling.
- Understanding and Using Transfer Learning for Security Tasks.
- Hands-on Lab: Building a Deep Learning Model for Advanced Intrusion Detection.

Unit Five: AI in Security Operations and Adversarial Machine Learning

- Automating Incident Response with AI and Security Orchestration (SOAR).
- Developing Predictive Threat Intelligence using Machine Learning.
- Understanding Adversarial ML: Evasion, Poisoning, and Extraction Attacks.
- Techniques for Defending ML Models against Adversarial Manipulation.
- Model Explain ability and Interpretability (XAI) in Cybersecurity.
- The Future of AI in Cyber Defense and Autonomous Security Systems.
- Capstone Project: Designing an End-to-End AI-driven Cyber Defense Strategy.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

As AI becomes more integrated into cyber defense, how do we balance automated decision-making with the need for human oversight and ethical judgment in critical security incidents?

What unique qualities does this course offer compared to other courses?

This course distinguishes itself by focusing on the practical application and strategic integration of AI and ML within a realistic cyber defense context. Unlike purely theoretical or data science-focused programs, our curriculum is built from the ground up by cybersecurity professionals for cybersecurity professionals. We bridge the critical gap between understanding an algorithm and knowing how to deploy it effectively to stop a real-world attack. The training emphasizes hands-on labs using security-specific datasets, allowing participants to grapple with the unique challenges of feature engineering and model tuning for threat detection and incident response. A significant portion of the course is dedicated to advanced, forward-looking topics such as adversarial machine learning, providing participants with both defensive and offensive perspectives on AI in security. This dual focus ensures a deeper, more robust understanding of the technology's vulnerabilities and strengths. Furthermore, the course structure promotes a strategic mindset, culminating in a capstone project where participants design a comprehensive AI-driven security framework, ensuring they leave not just with technical skills but with the vision to lead AI adoption in their organizations.