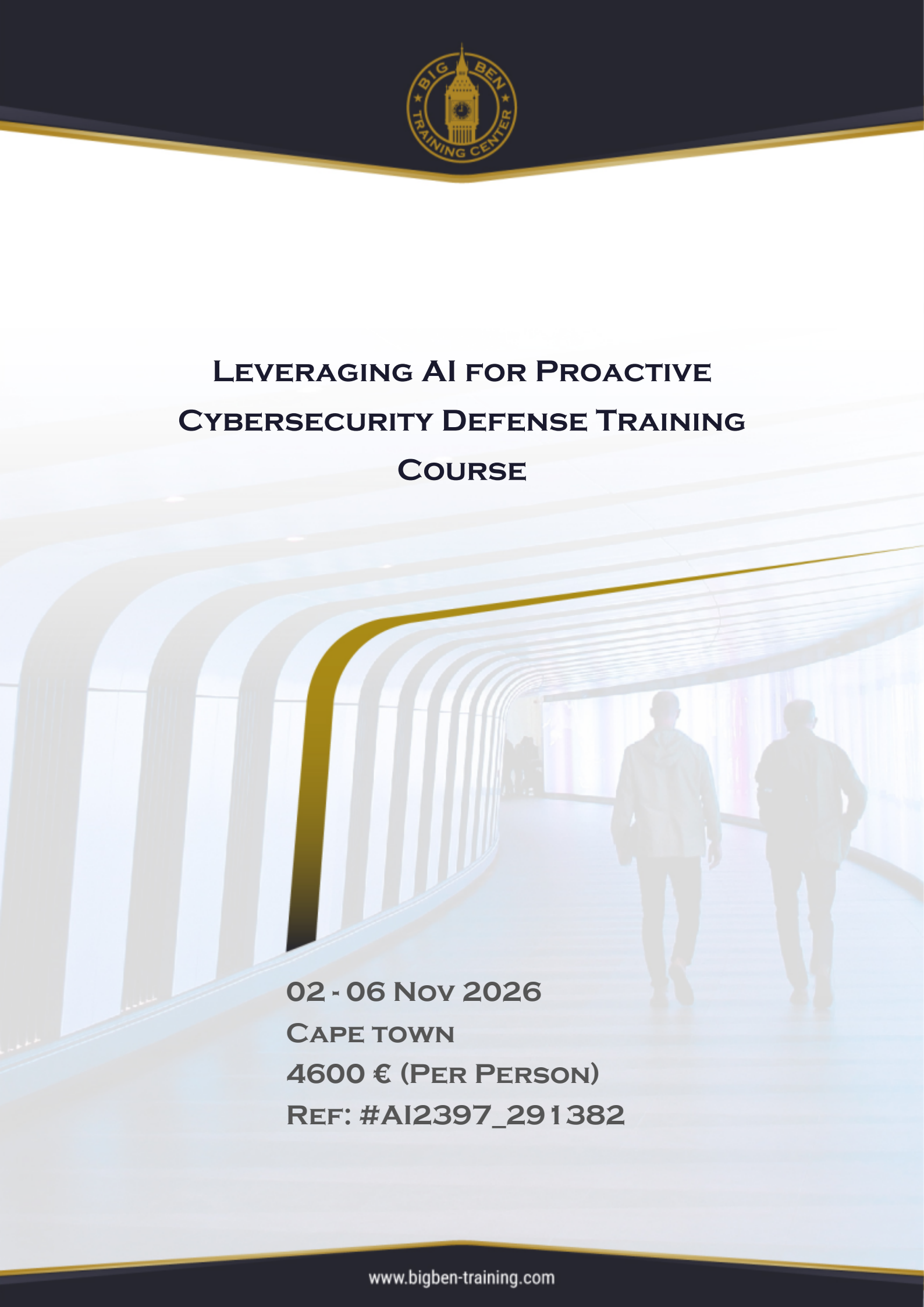
Leveraging AI for Proactive Cybersecurity Defense Training Course



02 - 06 Nov 2026

Cape town

4600 € (Per Person)

Ref: #AI2397_291382

Course Introduction / Overview:

This course provides a comprehensive exploration of the revolutionary intersection between Artificial Intelligence and cybersecurity. In an era of increasingly sophisticated digital threats, traditional defense mechanisms are often insufficient. This program is designed to equip professionals with the advanced knowledge and practical skills needed to leverage AI and machine learning for building proactive, intelligent, and resilient security infrastructures. We will delve into the core principles of AI-driven threat detection, predictive analytics, and automated incident response. As discussed by author Leslie F. Sikos in his work "AI in Cybersecurity", the integration of intelligent systems is no longer a futuristic concept but a present-day necessity for robust defense. Participants will move beyond theoretical understanding to practical application, learning how to implement AI models for tasks such as malware analysis, anomaly detection, and intelligent threat hunting. BIG BEN Training Center has developed this curriculum to bridge the critical gap between data science and security operations, empowering organizations to anticipate and neutralize threats before they escalate, thereby transforming their security posture from reactive to predictive.

Target Audience / This training course is suitable for:

- Cybersecurity Analysts and Engineers.
- Security Operations Center (SOC) Managers and Team Leads.
- IT Security Professionals and Administrators.
- Information Security Managers and Directors.
- Threat Intelligence Analysts.
- Data Scientists and Machine Learning Engineers moving into security.
- IT Auditors and Risk Management Professionals.
- Chief Information Security Officers (CISOs).

Target Sectors and Industries:

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

Target Organizations Departments:

- Information Technology (IT) Department.
- Information Security (InfoSec) Department.
- Security Operations Center (SOC).
- Risk Management and Compliance.
- Internal Audit.
- Research and Development (R&D).
- Data Analytics and Business Intelligence.
- Incident Response Teams.

Course Offerings:

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

- Develop a strategic framework for integrating AI into existing cybersecurity infrastructures.
- Apply machine learning algorithms for advanced threat detection and malware classification.
- Utilize Natural Language Processing (NLP) for analyzing security logs and threat reports.
- Implement AI-driven anomaly detection systems to identify suspicious network behavior.
- Design and deploy automated incident response workflows using AI and orchestration.
- Leverage predictive analytics to forecast potential cyber threats and vulnerabilities.
- Evaluate the challenges and ethical considerations of using AI in security.
- Defend against adversarial AI attacks designed to deceive security models.
- Enhance threat hunting capabilities with intelligent data analysis techniques.
- Formulate a forward-looking cybersecurity strategy based on emerging AI trends.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be highly interactive, engaging, and practical, ensuring that participants can immediately apply their learning in a real-world context. This course moves beyond traditional lectures by incorporating a blended learning approach that includes expert-led presentations, hands-on lab simulations, and collaborative group exercises. Participants will work with sanitized datasets to train machine learning models for tasks like intrusion detection and phishing analysis. A significant portion of the course is dedicated to the examination of detailed case studies, where we dissect high-profile cyberattacks and explore how AI-powered defenses could have altered the outcomes. Team-based workshops will challenge participants to design AI-driven security strategies for hypothetical organizations, fostering critical thinking and problem-solving skills. Continuous feedback is a cornerstone of our approach, with instructors providing personalized guidance throughout the sessions. This immersive and practical methodology ensures a deep and lasting understanding of how to leverage AI for proactive cybersecurity defense.

Course Agenda (Course Units):

Unit One: Foundations of AI and Machine Learning in Cybersecurity

- Introduction to Artificial Intelligence, Machine Learning, and Deep Learning.
- The Evolving Threat Landscape and the Need for Intelligent Defense.
- Core Applications of AI in Proactive Cybersecurity.
- Understanding Supervised, Unsupervised, and Reinforcement Learning for Security.
- Ethical Considerations and Bias in AI-Powered Security Systems.
- Key Performance Metrics for Evaluating AI Security Models.
- Setting up a Python Environment for Cybersecurity Data Science.

Unit Two: AI for Advanced Threat Detection and Analysis

- Machine Learning Algorithms for Intrusion Detection Systems (IDS).
- Deep Learning and Neural Networks for Malware Classification.
- Behavioral Biometrics and AI for User Authentication.
- Anomaly Detection in Network Traffic using Unsupervised Learning.
- Natural Language Processing (NLP) for Phishing and Spam Detection.
- Analyzing Security Logs and SIEM Data with AI.
- Practical Lab on Building a Simple Threat Detection Model.

Unit Three: Intelligent Threat Hunting and Predictive Analytics

- Transforming Threat Hunting from a Reactive to a Proactive Discipline.
- Using AI to Prioritize Alerts and Reduce Analyst Fatigue.
- Predictive Modeling for Identifying Potential Future Threats.
- Leveraging AI for Vulnerability Assessment and Prioritization.
- Graph Analytics and AI for Mapping Attack Paths.
- Integrating AI with Threat Intelligence Platforms.
- Case Study Analysis of an AI-assisted Threat Hunt.

Unit Four: Automated Incident Response and AI-Powered SOC

- Introduction to Security Orchestration, Automation, and Response (SOAR).
- Designing AI-driven Playbooks for Automated Incident Response.
- Leveraging AI to Accelerate Forensic Investigations.
- Building an AI-Powered Security Operations Center (SOC).
- The Role of AI in Digital Forensics and Incident Response (DFIR).
- Simulating an Automated Response to a Cyberattack.
- Future Trends in Security Automation and AI.

Unit Five: Adversarial AI and the Future of Cyber Defense

- Understanding Adversarial Machine Learning.
- Techniques for Attacking AI Security Models (Evasion, Poisoning).
- Developing Robust and Resilient AI Models Against Attacks.
- The Role of Generative AI in Both Offensive and Defensive Security.
- Building a Long-Term AI in Cybersecurity Strategy.
- The Future of AI, Quantum Computing, and their Impact on Security.
- Final Project Presentation on Designing an AI-Driven Security Framework.

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 might adversaries exploit the inherent trust we place in these automated systems, and what new paradigms of verification will be necessary?

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

This course distinguishes itself by moving beyond a purely theoretical or tool-specific approach to AI in cybersecurity. Instead, it focuses on building a strategic and conceptual understanding that empowers participants to design and implement bespoke AI-driven defense systems tailored to their organization's unique threat landscape. While other courses may focus on a single algorithm or platform, we emphasize the entire lifecycle of an AI security project, from data collection and model selection to deployment, monitoring, and defense against adversarial attacks. The curriculum is uniquely structured to bridge the gap between data science and security operations, providing cybersecurity professionals with the language of machine learning and data scientists with the context of security challenges. Our emphasis on proactive and predictive strategies, rather than just reactive detection, prepares participants for the next generation of cyber threats. The inclusion of extensive case studies and hands-on labs ensures that the knowledge gained is not just academic but deeply practical and immediately applicable to real-world security challenges.