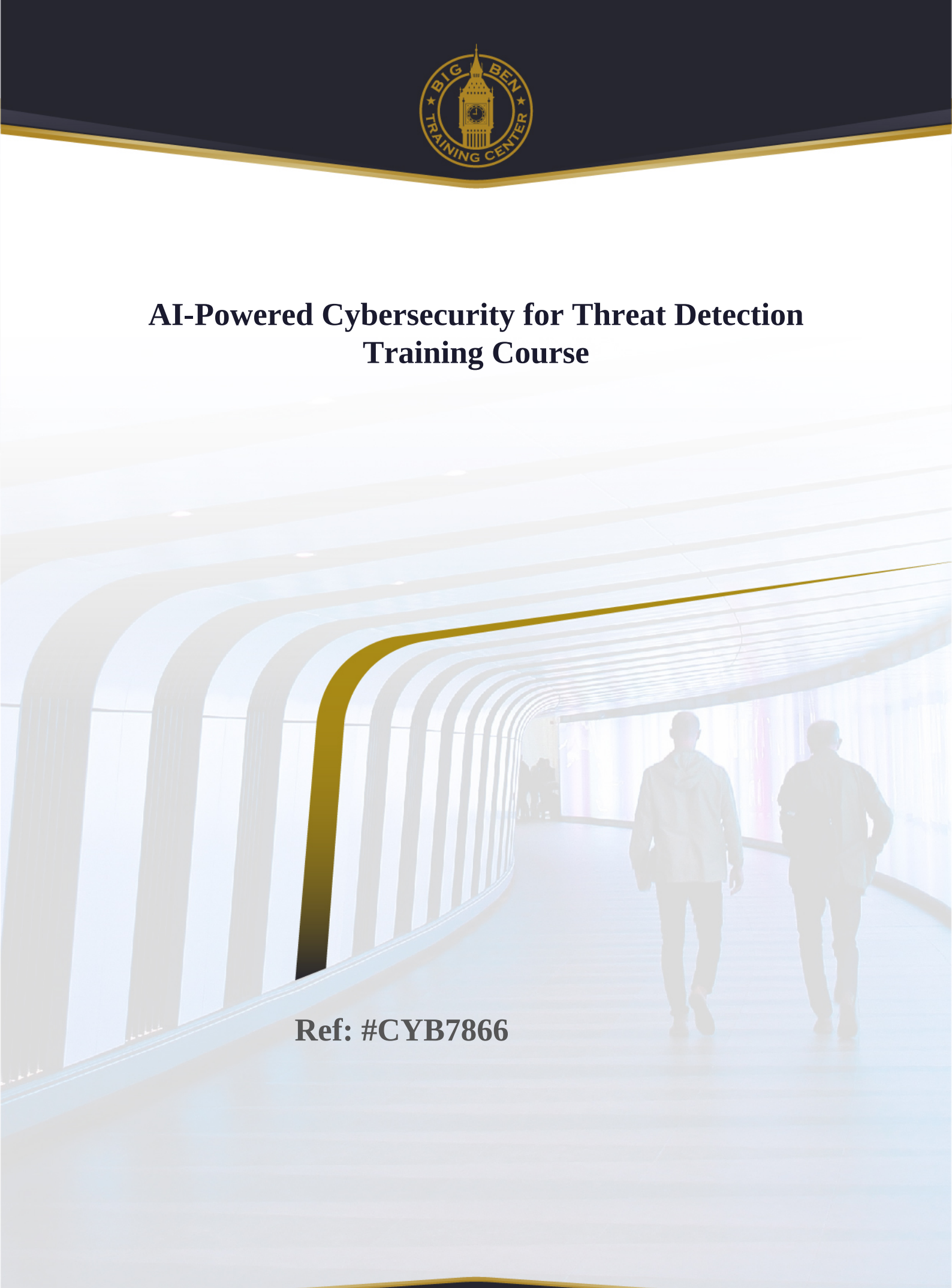
AI-Powered Cybersecurity for Threat Detection Training Course



Ref: #CYB7866

Course Introduction / Overview:

This comprehensive training course is designed to provide cybersecurity professionals with the advanced knowledge and skills required to leverage artificial intelligence (AI) for threat detection and response. The traditional methods of signature-based detection are no longer sufficient to combat the rapidly evolving landscape of cyber threats, especially those driven by sophisticated adversaries. This program goes beyond foundational security concepts to explore how machine learning, deep learning, and behavioral analytics can be used to identify anomalies and malicious activity in real time. Participants will learn how to implement AI-driven security tools, interpret their output, and build a proactive defense strategy that can adapt to new threats. Drawing from the academic work of renowned authors like Professor Wenliang Du and his book "Computer Security: A Hands-on Approach," this program provides a solid theoretical and practical framework. His work highlights the importance of understanding the underlying mechanics of security systems. This course at BIG BEN Training Center will empower you to integrate AI into your organization's security infrastructure and stay ahead of modern cyber threats.

Target Audience / This training course is suitable for:

- Cybersecurity analysts.
- Security operations center (SOC) staff.
- Threat intelligence analysts.
- Data scientists in cybersecurity.
- IT security managers.
- Network security engineers.
- Security architects.

Target Sectors and Industries:

- Financial services.
- Technology and software development.
- Government agencies and equivalents.
- Healthcare.
- Telecommunications.
- Managed security service providers.
- Consulting and professional services.

Target Organizations Departments:

- Information Security.
- Security Operations Center (SOC).
- Cybersecurity.
- IT Infrastructure.
- Risk Management.
- Threat Intelligence.
- Data Analytics.

Course Offerings:

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

- Explain the role of AI and machine learning in cybersecurity.
- Implement AI-driven tools for threat detection.
- Analyze security data using machine learning models.
- Develop a proactive, behavioral-based threat detection strategy.
- Integrate AI with a Security Information and Event Management (SIEM) system.
- Detect and respond to unknown or zero-day attacks.
- Evaluate the effectiveness of AI-powered security solutions.

Course Methodology:

This training course at BIG BEN Training Center uses a hands-on and data-driven methodology. The program combines expert-led lectures with a series of practical labs where you will work with real security data sets. You will learn to use open-source tools and platforms to build simple machine learning models for anomaly detection and malware classification. The course is structured around case studies of real-world attacks, allowing you to apply AI principles to uncover hidden threats. The instructor provides personalized feedback and guidance throughout the labs, ensuring that you not only understand the theory of AI but also its practical application in a security context. This approach ensures you will leave with the skills to effectively integrate AI into your security program.

Course Agenda (Course Units):

Unit One: Introduction to AI in Cybersecurity

- The evolution of cyber threats.
- The limitations of traditional security tools.
- Introduction to artificial intelligence and machine learning.
- Supervised vs. unsupervised learning for threat detection.
- Behavioral analytics vs. signature-based detection.
- The benefits of AI in a security operations center.
- Case study: a modern cyberattack.

Unit Two: Machine Learning for Threat Detection

- Data preparation for security analytics.
- Feature engineering and selection.
- Building and training a basic machine learning model.
- Classifying malware using machine learning.
- Detecting network anomalies and intrusions.
- Evaluating model performance (e.g., accuracy, false positives).
- Practical lab: a machine learning threat model.

Unit Three: AI-Powered Security Tools

- Overview of commercial AI security products.
- Integrating AI with SIEM and EDR platforms.
- Network traffic analysis with AI.
- User and Entity Behavior Analytics (UEBA).
- AI for phishing and email security.
- Automating incident response with AI.
- Case study: a UEBA implementation scenario.

Unit Four: Deep Learning and Advanced Techniques

- Introduction to deep learning.
- Using neural networks for threat detection.
- Natural Language Processing (NLP) for security.
- Graph analytics for identifying attack chains.
- Predictive analytics for threat forecasting.
- AI for vulnerability management.
- Practical lab: a deep learning model for threat detection.

Unit Five: The Future of AI and Cybersecurity

- Ethical considerations in AI security.
- The challenge of adversarial AI.
- Building a human-in-the-loop security program.
- Emerging trends in AI security.
- AI for security automation.
- Final project: a comprehensive AI security plan.
- The future of cybersecurity.
- Frequently Asked Questions:

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-driven systems become more sophisticated in detecting cyber threats, what are the ethical implications of using autonomous systems that make critical security decisions without human oversight or intervention?

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

This course stands out by providing a unique and essential focus on the application of artificial intelligence and machine learning in cybersecurity. Unlike many general security programs, this training moves beyond foundational concepts to address the advanced, data-driven methods required to combat modern threats. The curriculum is built around a hands-on approach. It teaches you how to work with real security data and build your own models for threat detection. This is not just a theoretical course. It gives you the practical skills to implement and manage AI-powered security solutions. The emphasis on practical labs, data analysis, and real-world case studies distinguishes this course from others. It is for security professionals who want to stay at the forefront of the industry and build a more intelligent, proactive defense strategy.