AI Security Deep Dive (TTAI2800)

Price: 2795

Duration: 3 days

Delivery Methods: Virtual

Overview

Overview

AI and machine learning systems introduce unprecedented security challenges that traditional cybersecurity practices cannot adequately address. **AI Security Deep Dive** delivers the specialized knowledge and hands-on experience needed to secure AI/ML systems against sophisticated attacks, protect sensitive training data, and implement robust defenses for AI-integrated applications. This intensive course is designed for programmers building AI-enabled applications, security analysts responsible for protecting AI systems, cybersecurity professionals expanding into AI security, and technical managers overseeing AI implementation projects.

Hands-On Format: – Days 1 and 2 feature interactive labs delivered via Jupyter notebooks, allowing participants to experiment directly with code, attacks, and defenses in a guided environment. – Day 3 focuses on real-world integration, exposing local models via a Flask API and integrating with a Large Language Model (LLM) using the Hugging Face Inference API (free tier, requires registration).

- Integration labs offer multiple language options: Python/Flask, Java/Spring, ASP.Net, and Node.js, so participants can choose the stack most relevant to their work.
- All labs and exercises are designed to be accessible with minimal setup, and detailed instructions are provided for each environment.

Throughout three intensive days, you will master the fundamentals of machine learning from a security perspective, identify and exploit vulnerabilities in AI systems through hands-on exercises, and implement practical defenses against data poisoning, adversarial attacks, and privacy

breaches. You will gain critical experience securing traditional applications that integrate AI models, including LLM-powered features, and learn to validate inputs and outputs to prevent prompt injection and other AI-specific attacks. The course combines essential AI/ML concepts with real-world security scenarios, ensuring you understand both the technical foundations and practical implementation challenges.

With a 50 percent hands-on approach, this course provides extensive practical exercises where you will simulate adversarial attacks, implement data poisoning defenses, conduct membership inference attacks, secure API integrations with AI models, and build comprehensive security strategies for AI-powered applications. Whether you are developing AI systems, securing existing implementations, or preparing for the next wave of AI-driven threats, you will leave with the expertise to protect machine learning applications, implement security-first AI development practices, and respond effectively to emerging AI security challenges.

Pre-Reqs

To ensure a smooth learning experience and maximize the benefits of attending this course, you should have the following prerequisite skills:

- Read code and understand basic programming concepts. The course provides hands-on opportunities using interactive Python and optionally other platforms. Successful students will need to setup a basic development environment, read and follow program logic and make minor modifications to code.
- Awareness of traditional cybersecurity issues. The successful student will have some prior knowledge of security issues in an IT environment.
- Basic understanding of web applications. Students should have some experience and exposure to basic HTTP based web technology.
- Familiarity with data handling and basic statistical concepts. Understanding of data formats, databases, and basic data analysis principles.
- Experience with software development lifecycle and security practices. Knowledge of testing, deployment, and security integration in development processes.

Course Schedule

Date	Time	Price	Options

06/22/2026	**09:00 AM - 05:00 PM CT**	**2,795.00**	**Buy Now Enroll**
08/10/2026	**09:00 AM - 05:00 PM CT**	**2,795.00**	**Buy Now Enroll**

Why Professional Choose TOPTALENT?

Dedicated Texas-Based Support

Get assistance every step of the way from our **Texas-based team**, ensuring your training experience is hassle-free and aligned with your goals.

3000+ Curated Professional Courses

Access an extensive portfolio of over 3000 courses across IT, Business Application and Leadership – Designed to meet evolving Industry demands

95% Client Approval Rating

Trusted by professionals nationwide our 95% approval rating reflects consistent quality, measurable impact and exceptional service.

Certified Industry Instructor

Learn from professionaly certified experts with real world experience and a proven commitment to learner success.

For questions

call:

(469) 721-6100

Email:

info@toptalentlearning.com

Find More Training

FAQ

What if I have to reschedule my class due to conflict?

Ten (10) business days' notice is required to reschedule a class with no additional fees. Notify TOPTALENT LEARNING as soon as possible at 469-721-6100 or by written notification to info@toptalentlearning.com to avoid rescheduling penalties.

How do I enroll for this class?

Please contact our team at 469-721-6100; we will gladly guide you through the online purchasing process.

What happens once I purchase a class?

You will receive a receipt and an enrollment confirmation sent to the email you submitted at purchase. Your enrollment email will have instructions on how to access the class. Any additional questions our team is here to support you. Please call us at 469-721-6100.

What is your late policy?

If a student is 15 minutes late, they risk losing their seat to a standby student. If a student is 30 minutes late or more, they will need to reschedule. A no-show fee will apply. Retakes are enrolled on a stand-by basis. The student must supply previously issued courseware. Additional fees may apply.

What happens when I finish my class?

You will receive a 'Certificate of Completion' once you complete the class. If you purchased an exam voucher for the class, a team member from TOPTALENT LEARNING will reach out to discuss your readiness for the voucher and make arrangements to send it.