AI Security Essentials for Non-Technical Professionals (TTAI2141)

Price: 995

Duration: 1 days

Delivery Methods: Virtual

Overview

Artificial intelligence is transforming business operations across every industry, but with this transformation comes new security risks that traditional cybersecurity approaches cannot fully address. **AI Security Essentials for Non-Technical Professionals** provides the foundational knowledge needed to understand AI security threats, recognize risks in your organization, and contribute to effective AI security strategies. This course is designed for professionals who interact with AI systems, manage AI projects, evaluate AI vendors, or need to understand AI security implications for their role.

Throughout this intensive day, you will develop a clear understanding of how AI systems work from a security perspective, learn to identify common AI-related threats and vulnerabilities, and understand the human factors that make AI security challenging. You will explore practical scenarios including deepfakes, AI-powered fraud, workplace AI tool usage, and vendor risk assessment. The course emphasizes real-world applications and provides immediately actionable knowledge that participants can apply in their daily work.

With a focus on practical understanding rather than technical implementation, this course provides case studies, demonstrations, and interactive discussions that help participants recognize AI security issues, ask the right questions when evaluating AI solutions, and contribute meaningfully to their organizationÃ¢â‚¬â„¢s AI security initiatives. Whether you are evaluating AI vendors, managing AI projects, or simply need to understand how AI impacts your organizationÃ¢â‚¬â„¢s security posture, you will leave with the knowledge to make informed decisions and recognize

potential security issues.

Objectives

By the end of this course, you will be able to:

- **Understand AI fundamentals from a security perspective.**
- **Identify common AI security threats and their business impact.**
- **Evaluate AI-related risks in workplace tools and vendor solutions.**
- **Recognize and respond to AI-powered social engineering and fraud.**
- **Contribute to AI security policy and incident response.**
- **Stay informed about emerging AI security trends.**

Audience

This **beginner-level** course is designed for non-technical professionals who need to understand AI security implications in their work. IT professionals, quality assurance teams, project managers, business analysts, security coordinators, and administrative professionals who interact with AI systems or influence AI adoption decisions will gain essential knowledge to contribute to their organizationÃ¢â‚¬â„¢s AI security posture.

Entry-level professionals entering IT or software engineering roles, managers overseeing AI projects, procurement professionals evaluating AI vendors, and compliance officers ensuring AI security adherence will also benefit from this foundational understanding. Whether you are directly working with AI systems, managing AI initiatives, or need to understand AI security risks in your organization, this course provides the essential knowledge without requiring technical programming or cybersecurity expertise.

Pre-Reqs

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

- **Basic computer literacy and familiarity with common software applications.** Comfort using email, web browsers, and standard business applications.
- **General understanding of business operations and organizational structures.** Awareness of how technology impacts business processes and decision-making.
- **Curiosity about technology and willingness to learn new concepts.** No technical background required, but openness to understanding how technology affects security and

business operations.

Course Schedule

Date	Time	Price	Options

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.