training code: AI Essentials v2 / ENG DL 2d NIS2 / EN

CompTIA AI Essentials v2 - Authorized training

CompTIA AI Essentials v2 is an authorized introductory course designed to help participants use artificial intelligence in a practical, informed, and responsible way in a professional environment.
The course is intended for individuals who want to understand the fundamentals of AI and learn how to use modern generative AI tools safely, responsibly, and in compliance with applicable regulations—without requiring advanced technical knowledge.
Participants will gain an understanding of how modern AI systems work, including generative models and chatbots, their practical applications in office and business settings, as well as the real limitations and risks associated with their use.
The program also addresses key topics such as ethics, information security, data protection, and compliance with major regulations and standards, including the EU AI Act, the NIST AI Risk Management Framework, and selected ISO/IEC standards.

The course provides a comprehensive introduction to generative AI, effective prompt design, critical evaluation of AI-generated outputs, and cybersecurity considerations related to modern AI-driven threats—including social engineering, OSINT, attack automation, and vulnerabilities in language models.
Version 2 places a strong emphasis on practical, job-ready AI skills. As a result, it is much better aligned with real business needs and prepares participants for the everyday use of generative AI tools in the workplace.

The CompTIA AI Essentials CompCert certification validates the acquisition of practical AI competencies and serves as a solid foundation for further professional development in artificial intelligence, cybersecurity, and emerging technologies.

NIS2 Directive

The NIS2 Directive expands the scope of EU cybersecurity regulations. Organizations covered by NIS2, as defined under national cybersecurity legislation, are required to implement products, services, or processes that comply with recognized certification schemes and security requirements.

Training recipients

This course is intended for individuals who want to use artificial intelligence tools consciously and effectively in their professional work, understand their real capabilities and limitations, and become familiar with the associated risks, responsibilities, and regulatory requirements.
The program is designed for both non-technical participants and those with basic IT experience.

The course is particularly recommended for:

- Professionals beginning to work with AI in a business environment who want to build solid, practical foundations for using generative AI without advanced technical skills.
- IT specialists and CompTIA learners, especially those who have completed or plan to complete certifications such as Security+, Network+, or CySA+, and wish to expand their skill set to include practical AI usage, security, and responsible adoption.
- Employees of organizations subject to NIS2, the AI Act, or other compliance requirements, who need to understand the impact of AI on information security, data protection, business processes, and organizational risk.
- Professionals in marketing, HR, sales, education, data analysis, and administration interested in using AI efficiently and securely in daily work, task automation, and decision support.
- Anyone who wants to use generative AI responsibly, with an emphasis on ethics, information security, regulatory compliance, and critical evaluation of AI-generated results.

Benefits

- Practical skills for working with generative AI
- Participants learn how to effectively use generative AI tools in everyday work, including crafting effective prompts, engaging in iterative AI interactions, and critically evaluating generated outputs.
- Responsible and informed use of AI
- The course develops an understanding of ethical, legal, and organizational aspects of AI usage,

including privacy protection, intellectual property, data processing, and compliance with regulations and internal policies.
- Secure use of AI in the workplace
- Participants gain insight into real-world AI-related threats, such as language model vulnerabilities, social engineering risks, and information security issues, along with practical approaches to mitigating these risks.
- Stronger foundation for further professional growth
- The training provides a solid base for continued development in artificial intelligence, cybersecurity, and modern technologies used within organizations.

Training program

1. Introduction to the Course and AI Competencies
   - Overview of the course structure and learning approach
   - Course objectives and competencies developed within AI Essentials v2
   - Initial self-assessment and identification of personal learning goals
   - Requirements and process for earning the CompTIA AI Essentials CompCert
2. Generative AI and the Fundamentals of Prompting
   - What generative AI is and how chatbots work
   - Practical differences between ML, LLMs, and GenAI—without technical jargon
   - Business and office use cases for generative AI tools
   - Limitations and risks of using AI
   - Core elements of effective prompting: purpose, context, persona, and constraints
   - Adapting prompts to specific tasks and using contextual files
3. Improving Output Quality and Handling AI Errors
   - What AI hallucinations are and why they occur
   - Types of errors in AI-generated responses
   - Methods for verifying and correcting AI outputs before use
   - Iterative interaction with AI instead of one-off prompts
   - Prompt chaining and refining results through dialogue
4. Responsible and Practical Use of AI at Work
   - Identifying situations where AI usage involves risk
   - Secure use of AI when handling sensitive or proprietary information
   - Responsible AI usage within organizations and alignment with internal policies
   - Knowing when to use AI—and when another tool is a better choice
   - AI as a teacher, creative partner, and productivity assistant
   - Basics of automating routine tasks with AI
5. Cybersecurity Risks and Threats Related to AI

- AI in reconnaissance, scanning, and attack automation
- Prompt injection, jailbreak techniques, and LLM vulnerabilities
- Password security in the age of AI
- AI-assisted OSINT
- AI in social engineering
- AI-driven attacks on web applications

6. Cybersecurity, Compliance, and AI Regulations

- Overview of AI regulations: EU AI Act, NIST AI RMF, ISO/IEC standards
- Challenges related to personal data and metadata protection
- Model documentation and Explainable AI (XAI)

Expected preparation of the participant

Participant Prerequisites

- Basic computer and office software skills
- General familiarity with computers, web browsers, and commonly used workplace tools is sufficient.
- Openness to new technologies and willingness to learn
- The course is designed for participants interested in exploring practical uses of AI and new ways of working with AI tools.
- Logical and critical thinking skills helpful for analyzing AI-generated responses, assessing their accuracy, and making informed decisions when using AI.

Training Includes

- 2 days of instructor-led training
- Instructor supervision and guidance
- Access to the learning community
- Electronic course materials
- Lab environment

Training Method

- Lecture
- Hands-on workshops

Duration

> 2 days / 14 hours

Language

Training: English
Materials: English