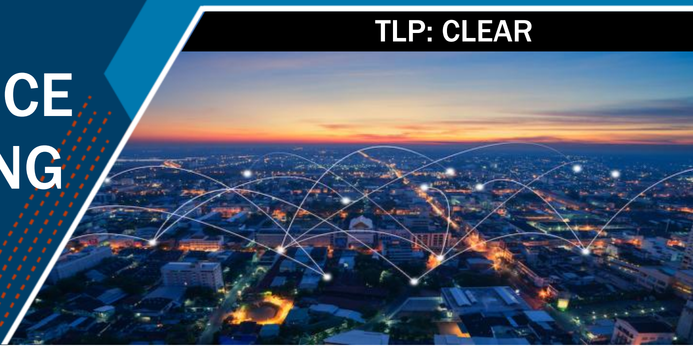
ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING PATHWAY



ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING PATHWAY

The **Artificial Intelligence and Machine Learning Pathway** is a comprehensive 4-week, instructor-led cybersecurity training course designed to build expertise in generative AI development. Starting with AI/ML fundamentals, participants progress through advanced architectures and cutting-edge applications while gaining hands-on experience with industry-standard tools and frameworks. The course emphasizes practical implementation of neural networks, natural language processing, and pre-trained models, culminating in the development of complete generative AI systems. By completion, students will gain fundamental skills to design, develop, and deploy AI applications that address real-world challenges while considering ethical implications and best practices.

KEY LEARNING OUTCOMES

- Process and prepare data for machine learning applications
- Implement basic Generative Adversarial Networks (GANs)
- Design effective prompt engineering strategies
- Design and implement end-to-end generative AI systems

CAREER OPPORTUNITIES RELATED TO THIS SUBJECT

- Machine Learning Engineer
- AI Developer
- Data Scientist
- AI Research Engineer
- NLP Engineer
- Computer Vision Engineer
- AI Solutions Architect
- ML Operations Engineer

PATHWAY METRICS

- Course Duration: 4-Weeks (160 hours)
- CPE Credits: 160
- Certification: AWS Certified AI Practitioner

This document is marked TLP: CLEAR. Recipients may share this information without restriction. Information is subject to standard copyright rules. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp.

PROFICIENCY LEVEL: INTERMEDIATE CYBERSECURITY PROFESSIONAL

Participants should have some technical exposure, ideally with basic programming (preferably in Python) and general familiarity with data concepts. While the course begins with foundational AI/ML concepts, it accelerates quickly into the implementation of neural networks, NLP, and generative models. Prior experience in artificial intelligence is not required, but comfort with coding and technical tools is essential for successfully navigating the course and engaging with the material. This course is not recommended for beginners.

TARGET AUDIENCE

This course is designed for individuals seeking to enter or advance within the AI/ML space, particularly with a focus on generative AI development. It is particularly suited for:

- Early-career data science, cybersecurity, or software development professionals looking to specialize in AI/ML
- Technologists or engineers with an interest in generative models, natural language processing, or machine learning
- Government personnel exploring AI/ML implementation in cybersecurity, threat intelligence, or automation
- Professionals preparing for the AWS Certified AI Practitioner exam or similar foundational AI certifications
- Individuals with some technical experience who are curious about applying AI in real-world use cases

RECOMMENDED PREREQUISITES:

While the prerequisites are not mandatory, they are essential for successfully navigating this course. This program is designed for individuals with a more robust understanding of IT and cybersecurity fundamentals—it is not recommended for beginners. If you lack a solid foundation in these areas, the course material may prove too challenging. All Pathway courses are live instructor-led to help facilitate learning and skill development for participants across broad skill levels.

To ensure readiness for the hands-on and technical aspects of the course, participants should ideally have the following exposure and proficiencies prior to enrolling:

- Basic proficiency with computers and operating systems (Windows/Linux), command-line navigation, and general understanding of file systems, folders, and application usage.
- Basic understanding of IT systems, including patch management, software updates, and common misconfigurations. *No prior experience in system hardening, vulnerability scanning, or deep operating systems knowledge is needed.*
- Comfort using basic command-line, including directory navigation, file operations, user commands, and introductory scripting capabilities. *No automation or tool-specific experience is required; however, it may be advantageous during training in lab environments*
- Familiarity with basic cybersecurity concepts including the CIA triad (confidentiality, integrity, availability), basic threat types (i.e., malware, phishing), software patching, and high-level understanding on security vulnerabilities.
- General understanding of networking concepts such as the OSI model (Open Systems Interconnection), IP addressing (Internet Protocol), and protocols like Transmission Control Protocol/ Internet Protocol (TCP/IP) and Hypertext Transfer Protocol (HTTP). *No prior exposure to packet analysis, protocol vulnerabilities, or secure network design is needed.*
- Basic Python programming experience, including writing and running simple scripts, using variables, functions, lists/dictionaries, and control flow (if/else statements, loops).
- Familiarity with foundational computing and data concepts, including data structures, files, application program interfaces (APIs), and basic data input/output (particularly in CSV/JSON formats). Participants should be comfortable using tools like NumPy, Pandas, and Jupyter, from the outset.
- Comfort navigating technical environments, installing software, using IDEs or notebooks. Participants will work extensively with Jupyter Notebooks, Python libraries, and cloud-based AI tools.
- Prior exposure to cybersecurity, data science, machine learning, and general awareness of AI applications.

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING COURSE OUTLINE

Week 1: The AI Foundation Builder: *A comprehensive introduction to AI/ML fundamentals, focusing on Python programming, neural networks, and NLP basics through hands-on implementation of essential concepts and tools.*

Week 1 Learning Outcomes:

- Configure a complete Python development environment for AI/ML applications
- Implement fundamental neural network architectures using Python
- Utilize essential ML libraries including NumPy and Pandas effectively
- Apply basic NLP concepts and techniques
- Process and prepare data for machine learning applications
- Explain core AI/ML concepts and their applications
- Execute basic neural network training procedures
- Demonstrate understanding of fundamental AI/ML mathematics

Week 2: The Generative Architecture Deep Dive: *An intensive exploration of modern generative AI architecture, focusing on GANs, VAEs, and Transformers through practical implementation and model fine-tuning exercises.*

Week 2 Learning Outcomes:

- Implement basic Generative Adversarial Networks (GANs)
- Work with Variational Autoencoders (VAEs)
- Utilize pre-trained language models like BERT and GPT
- Apply tokenization and embedding techniques
- Implement attention mechanisms
- Fine-tune pre-trained models for specific tasks
- Evaluate model performance and output
- Troubleshoot common training issues

Week 3: The Advanced Generation Explorer: *A practical immersion in advanced generative techniques, combining multimodal applications with ethical considerations through hands-on development of AI systems.*

Week 3 Learning Outcomes:

- Design effective prompt engineering strategies
- Implement few-shot learning techniques
- Develop multimodal AI applications
- Integrate text-to-image generation capabilities
- Apply style transfer techniques
- Identify and address ethical concerns in AI systems
- Implement bias detection and mitigation strategies
- Create responsible AI development workflows

Week 4: The Application Innovator: *An advanced study of real-world AI implementation, focusing on practical applications and system development through comprehensive project work.*

Week 4 Learning Outcomes:

- Design and implement end-to-end generative AI systems
- Create AI-powered content generation tools
- Develop conversational AI applications
- Build and deploy practical AI applications
- Integrate multiple AI technologies into cohesive systems
- Evaluating AI system performance and limitations
- Address real-world implementation challenges
- Present and document AI solutions professionally