Mastering Machine Learning Operations (MLOps) and AI Security Boot Camp - TTAI2810

Gain the hands-on skills required to automate, monitor, and secure machine learning workflows while boosting performance and reducing real-world AI risks.

Duration: 3 Days
Skill Level: Intermediate
Available Format: Instructor-Led Online; Instructor-Led, Onsite In Person ; Blended; On Public Schedule

In this hands-on and expert-guided course, you will explore the essential skills that help bring machine learning projects to life while keeping them secure and reliable. You will learn how to automate your machine learning workflows so that projects run smoothly and teams can collaborate with confidence. Along the way, you will practice monitoring and improving models, applying continuous integration, and managing risks in real time. You will also gain important skills in secure coding, learning how to protect your systems against threats that can harm performance and trust. From understanding how adversarial attacks work to building smart defenses, you will develop a toolkit you can use right away on the job. For those in leadership roles, you will learn how to guide your teams toward stronger governance, ethical practices, and safer use of AI across the organization. With every lab and discussion, you will gain a clearer sense of how to balance technical work with big-picture thinking. Whether you are hands-on with the code or overseeing projects, this course will help you become the person your team can count on to help make AI projects efficient, secure, and successful. You will leave with new skills and practical experience that will strengthen your role and make a real difference to your organization.

What You'll Learn

Overview

Artificial intelligence and machine learning operations (MLOps) are reshaping how organizations create, deploy, and protect their AI systems, and learning these skills puts you at the forefront of this transformation. This expert-led, three-day boot camp is designed to help you build the confidence and know-how to work with machine learning pipelines and secure AI systems in real-world settings. Whether you are a data scientist, machine learning engineer, DevOps specialist, cybersecurity professional, or a technical lead or manager overseeing AI projects, this course will help you strengthen your technical skills while gaining the bigger-picture perspective that organizations need today. With about 50 percent hands-on labs, you will not just hear about the techniques, you will practice them yourself.

Throughout the camp, you will learn how to design ML pipelines that are efficient, reliable, and ready for production, while also building a strong foundation in AI security. You will gain experience automating machine learning workflows to save time and reduce errors, setting up model monitoring to keep performance on track, and applying continuous integration and delivery to keep systems running smoothly. More importantly, you will understand why these practices matter — how they help teams work better together, avoid common pitfalls, and reduce the risks that can come from neglected models or poor version control. You will also build valuable skills in secure coding, learning how to protect systems against vulnerabilities, avoid adversarial attacks, and ensure that your AI integrations work safely inside web applications.

On the security side, you will explore how to think like a defender, identifying threats before they cause harm and creating action plans for incident response. You will also learn how to strengthen privacy, ethical practices, and governance around AI, helping you contribute not just as a technical expert but as a thoughtful leader on your team. Whether you are hands-on with the code or guiding AI projects from a leadership role, you will leave this course ready to help your organization improve the way it builds, deploys, and secures AI — adding value that goes far beyond the technology itself.

Objectives

The goal of this course is to help you build the confidence and skills to manage machine learning pipelines and secure AI systems in ways that truly make an impact. By the end of the course, you will be able to:

- Design and automate machine learning workflows that save time, reduce errors, and keep projects on track.
- Monitor and manage models effectively so you can quickly spot and fix performance issues before they affect results.
- Apply continuous integration and delivery practices to ensure smooth and consistent updates to your AI systems.

- Strengthen your secure coding skills to help protect systems from common vulnerabilities and risks.
- Identify and defend against AI threats like adversarial attacks, data poisoning, and prompt injection to keep systems safe.
- Develop practical strategies for managing AI risks, improving privacy practices, and guiding your team toward more secure and ethical AI use.

If your team requires different topics, additional skills or a custom approach, our team will collaborate with you to adjust the course to focus on your specific learning objectives and goals.

Audience

This course is designed for intermediate-level learners who want to deepen their technical skills in MLOps and AI security. It is a great fit for data scientists, machine learning engineers, DevOps professionals, IT security specialists, and technical leads or managers who support AI projects. To get the most from this course, you should have some hands-on experience with machine learning and basic familiarity with cloud services or programming.

Skills-Based Pre-Reqs:

1. A solid understanding of machine learning fundamentals such as supervised and unsupervised learning and basic model building.
2. Basic Python programming experience and comfort working with data analysis tasks.
3. Familiarity with general cybersecurity principles and cloud or DevOps workflows.

Pre-Requisites

To get the most out of this course, you should have experience with:

- Machine Learning Fundamentals. Understanding of supervised and unsupervised learning, model training, and evaluation techniques.
- Python Programming for Data Science. Ability to write and modify Python scripts, work with libraries like Pandas and NumPy, and preprocess data for machine learning.
- Basic Cloud and DevOps Concepts. Familiarity with cloud platforms (AWS, Azure, or GCP), version control (Git), and workflow automation principles.

Take Before: In order to gain the most from this course, you should have incoming skills equivalent to those in the course listed below, or should have attended this as a prerequisite:

TTML5502	Exploring AI & Machine Learning for the Enterprise Overview (Light Hands-on)
TTPS4873	Fast Track to Python for Data Science and/or Machine Learning

Agenda

Please note that this list of topics is based on our standard course offering, evolved from current industry uses and trends. We will work with you to tune this course and level of coverage to target the skills you need most. Course agenda, topics and labs are subject to adjust during live delivery in response to student skill level, interests and participation. The course tools, topics, use cases and hands-on labs can also be easily adjusted to suit your specific needs, goals or requirements. Please inquire for details and options.

Introduction to MLOps

Learn why MLOps matters and how it connects data science and operations to bring machine learning models smoothly into real-world use.

- MLOps: The key to integrating data science with operations for AI model efficiency
- Understanding the need for MLOps
- Differences between MLOps, DevOps, and DataOps
- MLOps lifecycle overview

MLOps Tools and Techniques

Get familiar with the key tools and practices that help you build, manage, and improve machine learning pipelines with confidence.

- Review essential tools and practices for building effective and sustainable ML pipelines
- Overview of MLOps tools (MLflow, Kubeflow, etc.)
- MLOps pipeline components
- MLOps best practices
- Walking through a simple machine learning pipeline

Automating Machine Learning Workflows

Discover how to save time and improve results by automating important steps in your machine learning workflows.

- Explore the importance of automating ML workflows for improved efficiency and model deployment
- The role of automation in MLOps

- Continuous Integration and Continuous Deployment (CI/CD) in machine learning

Model Monitoring and Management

Find out how to keep an eye on your models, catch performance issues early, and keep them running at their best.

- Understanding model decay and why it matters
- Continuous performance monitoring and anomaly detection
- Data drift and concept drift analysis
- Implementing feedback loops for continuous improvement
- Learn how to track, organize, and safely update your models so you always know what's running in production.

MLflow in Practice

See how to use MLflow to log, compare, and fine-tune your experiments, making it easier to learn what works and what doesn't.

- Setting up MLflow tracking servers and UI
- Organizing experiments, runs, and hyperparameter tuning
- Capturing parameters, metrics, and artifacts
- Visualizing and comparing experiment results

Orchestration and Pipelines

Explore how to design smart, automated pipelines that help your machine learning projects run smoothly and reliably.

- Understanding the role of orchestration in MLOps
- Setting up workflows and pipelines using tools like Prefect
- Adding retries, notifications, and caching
- Enabling collaboration across teams and workflows

Foundations of AI and Secure Coding

Understand the basics of AI and why secure coding is critical when building or working with AI-powered applications.

- Exploring the intersection of AI and software security
- Key concepts: machine learning, deep learning, LLMs, generative AI
- Real-world examples of AI in web applications

- Why AI awareness matters for secure coding and design

Secure Coding Principles in the Age of AI

Learn how to write and check code that keeps AI systems safe from common and emerging risks.

- Identifying AI-specific coding vulnerabilities
- Applying OWASP principles to AI systems
- Securing data pipelines, model inputs, and outputs
- Implementing output constraints and validation

How AI Attacks Your Code, Systems, and Teams

See how attackers use AI to find weak spots—and how you can recognize and reduce these risks.

- Understanding AI-powered attack techniques
- Prompt injection, data poisoning, and model evasion
- Risks from AI-generated code and API abuse
- Human-in-the-loop risks and social engineering amplification

Defending Against AI-Powered Attacks

Build practical strategies for protecting your systems and data from AI-driven threats.

- Building AI-aware threat models
- Mapping risks to practical defenses and controls
- Monitoring and logging for AI systems
- Tools and strategies for securing the software supply chain

Secure AI Integration in Web Applications

Learn how to safely connect AI models to your web applications without adding new security holes.

- Managing risks of integrating AI in web apps
- Securing API interactions and data protection
- Validating and sanitizing inputs and outputs
- Avoiding common integration pitfalls

Natural Language Processing (NLP) and AI Security Risks

Understand the unique risks that come with NLP tools and how to use them safely in your work.

- Understanding NLP and its widespread use
- Mitigating prompt injection, data leakage, and context hijacking
- Using NLP tools responsibly in security workflows
- Implementing safeguards for NLP models in production

AI Risk Management and Security Leadership

Discover how to guide teams and organizations toward smart, responsible, and secure AI use.

- Applying governance frameworks to manage AI risk
- Incorporating AI into the secure development lifecycle (SDLC)
- Establishing guardrails and policy approaches
- Evaluating AI tools and leading responsible adoption

Bonus: Staying Safe with AI Tools at Work

Pick up practical tips to help yourself and your team use popular AI tools safely and responsibly on the job.

- Recognizing risks of workplace AI tools (e.g., ChatGPT, Copilot)
- Best practices for safe AI use on the job
- Protecting data, intellectual property, and organizational reputation
- Tips for guiding teams on responsible AI adoption

Addendum: Resources, Insights & Tip Guides

Follow On Courses

TTAI2835	AI & Web Application Security: A Practical Guide to Risks & Responses
TTAI2830	Applying AI to the 2021 OWASP Top Ten
TTML5517	MLOps Boot Camp | ML in Action: Deploy, Monitor, and Master

Related Courses

TT8320-J	Java Secure Coding Camp | Attacking and Securing Java Web Applications

TT8700	Securing Databases: Practical Database Security Skills for Safer Systems
TTAI2820	Mastering AI Security Boot Camp
TTPS4894	Python Security | Introduction to Python Programming for Security Analysts & Professionals
TTAI2830	Applying AI to the 2021 OWASP Top Ten
TTML5517	MLOps Boot Camp | ML in Action: Deploy, Monitor, and Master
TT8120	Web Application Security Essentials: Understanding OWASP Risks and Fixes That Really Work
TT8320-N	.Net Secure Coding Camp | Attacking and Securing C# / ASP.Net Core Web Applications
TTAI2835	AI & Web Application Security: A Practical Guide to Risks & Responses

Setup Made Simple! All of our course software, digital course files or course notes, labs, data sets and solutions, live coaching support channels and rich extended learning and post training resources are provided for you in our easy access, single source, no install required online Learning Experience Platform (LXP), remote lab and content environment. Or we can provide a local installation (trial edition) to setup and use on your machine. Access periods and versions vary by course. Please inquire about set up details and options for your specific course of interest. Regardless of setup option, we will collaborate with you to ensure your team is set up and ready to go well in advance of the class.

Ways to Learn: At Trivera, we believe that Experience is Everything. Our customizable, hands-on courses are delivered live online, onsite, or in a blended format for maximum flexibility. We provide real-time expert-led training and coaching for all skill levels, from small groups to enterprise-wide programs, ensuring every learner gains the latest, most relevant job-ready skills they can apply with confidence. This course is also available for individuals or small groups on our extensive Public Schedule (see current dates below). We look forward to helping you take the next steps in your modern web developer learning journey.

For More Information

Please contact us or call 844-475-4559 toll free for more information about our training services (instructor-led, self-paced or blended), coaching and mentoring services, public course enrollment or questions, partner programs, courseware licensing options and more.