Mastering AI Security Boot Camp - TTAI2820

Hands-on AI Security | Essentials, Threat Detection, Vulnerabilities, Forensics, Incident Response & Future Trends

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

The **Mastering AI Security Boot Camp,** a three-day course geared for technical users keen to explore the intersection of artificial intelligence and cybersecurity. With AI transforming the cybersecurity landscape, a deep understanding of AI in security can enhance your efficiency in tackling security issues, formulating defense strategies, and fortifying your organization's security stance.

What You'll Learn

Overview

Artificial intelligence is transforming cybersecurity, both as a tool for protection and as a target for emerging threats. **Mastering AI Security Boot Camp** provides the hands-on skills needed to analyze AI-driven threats, secure machine learning models, and implement defense strategies that safeguard organizations from evolving attacks. This expert-led, interactive course is designed for cybersecurity professionals, data scientists, system administrators, AI engineers, and IT leaders who need to understand and mitigate the unique security risks associated with AI technologies. Technical managers, project leads, and compliance professionals overseeing AI security initiatives will also gain critical insights into risk management, ethical AI security practices, and incident response strategies.

Over three days, you will identify vulnerabilities in AI systems, apply intrusion detection techniques, and strengthen machine learning models against adversarial threats. You will develop practical skills to analyze security incidents, conduct forensic investigations on AI systems, and build response plans that minimize the impact of cyber threats. The course also explores differential privacy, ethical considerations, and the role of AI in cybersecurity automation, ensuring you can balance protection with responsible AI use.

With a 50 percent hands-on approach, this course provides real-world exercises where you will simulate AI security attacks, implement defense strategies, and assess AI-driven security risks in practical scenarios. Whether you are actively securing AI systems or guiding AI adoption within your organization, you will leave with the knowledge and skills to protect machine learning applications, strengthen cybersecurity postures, and respond effectively to AI-related security challenges.

Objectives

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

- **Detect and analyze AI security threats.** Identify vulnerabilities in machine learning models, recognize adversarial attack methods, and assess risks to AI-driven systems.
- **Implement AI-specific intrusion detection and defense strategies.** Use AI-powered security tools to safeguard data, models, and networks from evolving cyber threats.
- **Develop forensic analysis skills for AI systems**. Investigate AI-related security breaches, trace attack vectors, and apply forensic techniques to compromised models.
- **Design and execute AI incident response plans.** Build structured response strategies to mitigate security threats and reduce the impact of AI-driven cyber incidents.
- **Enhance AI privacy and ethical security practices.** Apply differential privacy, encryption, and ethical guidelines to secure AI applications while ensuring compliance.
- **Prepare for future AI security challenges**. Stay ahead of emerging risks, such as deepfake manipulation, AI-driven cyberattacks, and AI security automation trends.

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 **intermediate-level** course is designed for cybersecurity professionals, AI engineers, system administrators, and data scientists who need to secure machine learning systems and mitigate AI-driven threats. Individuals in threat analysis, incident response, and IT security roles will gain essential skills to detect vulnerabilities and build AI-specific defense strategies.

Technical managers, compliance professionals, and project leads overseeing AI security initiatives will also benefit from this course by gaining insights into governance, ethical AI considerations, and incident response frameworks. Whether you are directly securing AI systems or ensuring AI security compliance, this course equips you with the expertise to manage risks, strengthen security strategies, and build resilient AI-driven security solutions.

Pre-Requisites

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

- A foundational understanding of artificial intelligence, including the basic principles, applications, and types of AI.
- Familiarity with basic cybersecurity principles, understanding of threats, defense mechanisms, and incident response.
- Basic Python programming skills and / or a general comfort with coding
- Basic knowledge of computer networks, systems, and how they interact
- Some basic experience in data analysis or basic statistical concepts.

TT8120	Web Application Security Essentials: Understanding OWASP Risks and Fixes That Really Work
TTAI2835	AI & Web Application Security: A Practical Guide to Risks & Responses
TTML5502	Exploring AI & Machine Learning for the Enterprise Overview (Light Hands-on)
TTML5503	Introduction to AI & Machine Learning JumpStart
TTPS4800	Introduction to Python Programming Basics

Agenda

Please note that this list of topics is based on our standard course offering, evolved from typical industry uses and trends. We will collaborate with you to tune this course and level of coverage to target the skills you need most. Topics, agenda and labs are subject to change, and may adjust during live delivery based on audience skill level, interests and participation.

Introduction to AI in Security

Explore foundational AI security, threat identification, and protective strategies through practical examples.

- The Need for AI Security
- Exploring AI Threat Landscape
- Identify Threats and Implement Protections in AI Systems
- Implement AI Security Best Practices
- Top Ten Pitfalls to Avoid
- Activity: Implementing Basic Security Measures
- Benefits of Applying AI to Cybersecurity

Playing Detective: Identifying AI Threats and Vulnerabilities

Explore AI system vulnerabilities, different threat types, and data privacy concerns

- Inherent threats and vulnerabilities of AI systems
- Different types of AI threats
- Common AI vulnerabilities
- Case studies of major AI-based security breaches

Building the AI Fortress: Defense Mechanisms 101

Learn how to design and implement robust AI-driven defense systems.

- Safeguard AI systems from security threats.
- Deep Dive AI Security Measures
- AI Defense Mechanisms
- AI in intrusion detection and prevention systems
- AI in risk assessment and vulnerability management
- Activity: Design a basic AI-driven Intrusion Detection System

AI Adversarial Attacks and Defenses

Learn how to tackle adversarial threats to AI systems with effective defense strategies for security.

- Adversarial attacks Deep Dive
- Techniques to defend against adversarial attacks
- Implementing defense measures against sample adversarial attacks

- Activity: Defending Against Adversarial Attacks

CSI Cyber: A Foray into AI Forensics

Apply forensic techniques and analyzing AI security incidents.

- How forensic techniques are applied in AI security.
- Role of forensics in AI Security
- Basics of AI Forensic Analysis
- Case studies of forensic analysis in AI security incidents
- AI in forensic data analysis
- Activity: Conduct a simple forensic analysis on an AI system

Crisis Averted: Crafting Your AI Incident Response Plan

Develop and execute effective incident response plans for AI system breaches

- How to respond to incidents in AI systems effectively.
- Basics of Incident Response (IR) in AI systems
- AI in IR: Automated and adaptive response
- Designing an incident response plan for AI systems

AI Privacy and Ethical Considerations

Address privacy risks and ethical considerations in AI applications

- Navigate privacy and ethics in AI to promote responsible technology use.
- Privacy risks in AI/ML applications
- Understanding differential privacy
- Ethical considerations in AI Security
- Hands-on Lab: Implementing differential privacy in a machine learning model

What's Next? Preparing for Future AI Security Challenges

Explore future AI security trends and prepare for emerging threats.

- Get insights into the future trends of AI in cybersecurity.
- Future threats: Deepfakes, autonomous weapons, etc.
- AI in quantum computing security

- AI-driven Security Orchestration, Automation, and Response (SOAR)
- The role of AI in zero-trust architectures

Bonus Chapters / Addendum

- Next steps in Your AI Security Journey
- Ethical AI Deeper Dive - Implementing Ethical AI in Everyday Business Practices
- Everyday AI Security: Staying Safe and Smart with AI Tools

Addendum / Resources

- Course Site References & Additional Information
- Glossary of Main Terms, Skills and Key Topics
- Next Steps, Follow on Courses & SkillJourneys

Related Courses

TT8320-J	Java Secure Coding Camp | Attacking and Securing Java Web Applications
TT8700	Securing Databases: Practical Database Security Skills for Safer Systems
TT8120	Web Application Security Essentials: Understanding OWASP Risks and Fixes That Really Work
TTAI2810	Mastering Machine Learning Operations (MLOps) and AI Security Boot Camp
TTAI2835	AI & Web Application Security: A Practical Guide to Risks & Responses

All applicable course software, digital courseware 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, no install required” online **Learning Experience Platform (LXP),** remote lab and content environment. Access periods vary by course. We’ll collaborate with you to ensure your team is set up and ready to go well in advance of the class. Please inquire about set up details and options for your specific course of interest.

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.