AI & Machine Learning Security Series

Mastering AI Security Boot Camp (TTAI2820)

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

Course Snapshot

- **Course: Mastering AI Security Boot Camp (TTAI2820)**
- **Duration**: 3 days
- **Audience & Skill Level:** The intermediate and beyond level course is a great fit for technical professionals eager to deepen their knowledge in machine learning and AI security. Roles include Data Scientists, Machine Learning Engineers, IT Security Professionals, and DataOps Engineers or similar.
- **Format / Hands-on:** This course combines engaging instructor-led presentations and practical demonstrations with hands-on exercises, challenge labs, use case exploration and engaging group activities. Student machines are required.
- **Flexible Delivery Options**: This course can be delivered for your team or organization **online-live (virtual)**, **onsite in-person, self-paced** or across our immersive **blended learning experience platform (LXP).**
- **Public Schedule**: This course is currently available on our Public Open Enrollment Schedule.
- **Customizable**: We're flexible! This course agenda, topics, labs, hours and delivery modalities can be adjusted to target your specific training skills objectives, tools and learning goals. Please ask for details.

Description

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. Whether you're tackling security issues, designing advanced defense mechanisms, or simply looking to stay ahead of the curve, these skills can streamline your daily tasks and significantly contribute to your organization's security posture.

Working in a hands-on learning environment guided by our AI security expert, you'll explore AI in cybersecurity, AI threats and vulnerabilities, defense mechanisms, forensics, incident response for AI systems, and future trends in AI security. You'll gain an understanding of AI's role in security and threat intelligence, enabling you to better predict and understand emerging threats, resulting in proactive rather than reactive defense strategies. You'll also learn about AI vulnerabilities and their mitigation. Identifying potential weaknesses in AI systems allows for more robust security measures, reducing the risk of breaches. You'll also master incident response for AI systems. Handling security incidents effectively can drastically reduce the potential damage caused by breaches, ensuring business continuity.

The hands-on labs are designed to provide real-world scenarios that simulate challenges faced in the field. You will be analyzing AI-driven threats, identifying vulnerabilities in AI systems, designing an AI-driven Intrusion Detection System, conducting a basic AI forensic analysis, and developing an incident response plan for an AI system. Tools and skills used in the class include Python, Scikit-learn and open-source threat intelligence platforms. Upon completing the course you'll be well equipped to understand and mitigate AI threats, design and implement AI defense systems, and effectively respond to incidents in AI systems.

Learning Objectives

Throughout the course you'll:

- Gain a clear understanding of AI and its integral role in the realm of cybersecurity, providing a solid foundation for the rest of the course.
- Learn to identify and understand various types of AI threats and vulnerabilities, improving your ability to predict and mitigate potential risks.
- Acquire the knowledge to design and implement robust AI defense mechanisms and AI Driven Intrusion Systems (IDS), equipping you to safeguard your systems effectively.

- Delve into the fascinating world of AI forensics and learn how to conduct basic forensic analyses on AI systems.
- Master the art of creating and executing incident response plans for AI systems, a vital skill for any security professional.
- Learn specific techniques to detect deepfakes and understand their potential security implications, equipping you to counter one of the emerging threats in the AI security landscape.
- Get hands-on experience with innovative open-source tools such as Python, Scikit-learn, and Suricata IDS, enhancing your ability to use these tools effectively in AI security.
- Get insights into future trends in AI security, ensuring that you're well-prepared for what's around the corner in this rapidly evolving field.

Audience

This intermediate-level course is a fit for experienced cybersecurity professionals, system administrators, developers and IT managers seeking to enhance their understanding of artificial intelligence in the context of security. Individuals in roles responsible for threat analysis, incident response, and system defense will find the course particularly beneficial.

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.

Take Before: Students should have incoming practical skills aligned with those in the course(s) below, or should have attended the following course(s) as a pre-requisite:

- TTML5502 Exploring AI & Machine Learning Overview / Hands-On (2 days)
- TTPS4800 Introduction to Python Programming Basics (3 days) (Helpful but not required)

Next Steps / Follow-on Courses: We offer a wide variety of follow-on courses and learning paths for Generative AI, AI for Business, GPT, Applied AI, Azure OpenAI, Google BARD, AI for developers, testers, data analytics, machine learning, deep learning, programming, intelligent automation, AI Security and many other related topics. Please see our catalog for the current **AI & Machine Learning Courses, Learning Journeys & Skills Roadmaps**, list courses and programs.

Course Topics / Agenda

Please note that this list of topics is based on our standard course offering, evolved from typical industry uses and trends. We'll work 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.

1. **Introduction to AI in Security**

- Understand the role of AI in the field of cybersecurity and the evolution of threats.
- The basics of AI and its relevance to security
- Cybersecurity landscape: traditional threats vs. AI-enabled threats
- Real world examples of AI in security
- Understanding the role of AI in Threat Intelligence
- Lab: Simulating AI-driven threat analysis using open-source threat intelligence tools

2. **Playing Detective: Identifying AI Threats and Vulnerabilities**

- Grasp the inherent threats and vulnerabilities of AI systems
- Understanding the different types of AI threats
- Learning about common AI vulnerabilities
- Exploring case studies of major AI-based security breaches
- AI and data privacy concerns
- Lab: Identifying vulnerabilities in an AI system (2:30 - 4:00)
- Tools Used in Lab: Python, Scikit-learn, OWASP Dependency-Check

3. **Building the AI Fortress: Defense Mechanisms 101**
- Gain knowledge on how to safeguard AI systems from security threats.
- Importance of AI Security Measures
- Learning about AI Defense Mechanisms
- AI in intrusion detection and prevention systems • AI in risk assessment and vulnerability management
- Lab: Designing a basic AI-driven Intrusion Detection System

4. **CSI Cyber: A Foray into AI Forensics**
- Understand how forensic techniques are applied in AI security.
- The 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
- Lab: Conducting a simple forensic analysis on an AI system

5. **Crisis Averted: Crafting Your AI Incident Response Plan**
- Learn 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
- Lab: Creating a mock incident response plan for an AI system

6. **What's Next? Preparing for Future AI Security Challenges**
- 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
- Lab: Simulating the detection of a deepfake

Course Wrap
- Next steps in becoming an AI Security Expert

Setup Made Simple! Learning Experience Platform (LXP)

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

For more information about our training services (instructor-led, self-paced or blended), collaborative coaching services, robust Learning Experience Platform (LXP), Career Experiences, public course schedule, partner programs, courseware licensing options or to see our complete list of course offerings, solutions and special offers, please visit us at **www.triveratech.com**, email **Info@triveratech.com** or call us toll free at **844-475-4559.** Our pricing and services are always satisfaction guaranteed.