Mastering AI Security Boot Camp - TTAI2820

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

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. 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.

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

TTML5502	Exploring AI & Machine Learning for the Enterprise Overview (Light Hands-on)
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'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.

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

Follow On Courses

{{code}} {{title}}

Related Courses

TT8120	Securing Web Applications | 2021 OWASP Top Ten and Beyond
TT8320-J	Java Secure Coding Camp | Attacking and Securing Java Web Applications
TT8700	Securing Databases | Database Security

Attend a Course

Please feel free to Register Online or call 844-475-4559 toll free to connect with our Registrar for assistance. If you ever need additional date options, please contact us for scheduling.