Skillsoft
global knowledge™

# MASTERING AI SECURITY BOOT CAMP

Course Code: 840018

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

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.

## What You'll Learn

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.

## Who Needs to Attend

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.

## Prerequisites

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.

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 6/22/2026 12:13:41 PM