

AI in Cybersecurity: Tools & Techniques for Professionals

29 March – 2 April 2027
Rome

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

AI in Cybersecurity: Tools & Techniques for Professionals

Ref: 103600542_81669 **Date:** 29 March – 2 April 2027 **Location:** Rome **Fees:** 5700 Euro

Course Overview:

In today's rapidly evolving cybersecurity landscape, Artificial Intelligence AI is playing an increasingly pivotal role. This course, "AI in Cybersecurity: Tools & Techniques for IT Professionals," offers IT security professionals and engineers the knowledge and tools needed to defend against the growing threats facilitated by increasingly sophisticated cybercriminals. By integrating AI with cybersecurity, participants will explore advanced methodologies like machine learning, predictive analytics, and autonomous defense strategies, aimed at enhancing their cybersecurity posture. AI-powered systems bring automation, smarter decision-making, and near-instant threat detection to the forefront of IT security. Upon completion, attendees will be equipped to apply AI in threat detection, prevention, and real-time defense operations.

Target Audience:

- IT Security Engineers
- Cybersecurity Analysts
- IT Professionals focusing on cybersecurity
- Network Security Specialists
- Data Protection Officers
- IT Managers with a focus on Cyber Defense
- Security Operations Center SOC Analysts

Targeted Organizational Departments:

- IT Security
- Network Operations
- Cyber Defense
- Incident Response Teams
- Risk Management
- Compliance & Data Privacy Teams

Targeted Industries:

- Information Technology & Cybersecurity
- Finance & Banking
- Government & Defense
- Healthcare for data protection
- Telecommunications
- E-Commerce & Online Platforms

Course Offerings:

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

- Understand AI fundamentals and how they apply to cybersecurity.
- Implement machine learning techniques to enhance threat detection.
- Use AI for predictive analytics in network security.
- Apply AI-powered tools to automate threat responses.
- Utilize AI techniques in cybersecurity defense systems to secure networks.
- Detect adversarial threats through advanced AI algorithms.
- Understand the importance of securing AI systems within cybersecurity protocols.

Training Methodology:

This course will incorporate a blend of theoretical sessions, case studies, and interactive discussions. Participants will engage with the material through group work, where they will collaborate on solving real-life cybersecurity problems, and review case studies that examine previous cybersecurity breaches. These case studies will highlight how AI could have been applied to mitigate such incidents, offering valuable insights into the practical application of AI in cybersecurity. Additionally, interactive demonstrations will allow participants to explore the role of AI tools in identifying security threats, all while benefiting from continuous feedback and tailored guidance throughout the course. This approach ensures a comprehensive understanding of AI's impact on cybersecurity and equips participants with the knowledge to apply AI techniques in their professional environments.

AGILE LEADERS
Training Center

Course Toolbox:

- AI-based cybersecurity tools demo versions
- Access to predictive analytics dashboards
- Case study templates
- Online resources and reading materials, including relevant whitepapers and research articles
- Checklist for implementing AI in cybersecurity measures

Course Agenda:

Day 1: Introduction to AI in Cybersecurity

- **Topic 1**: Fundamentals of AI and Machine Learning in Cybersecurity
- **Topic 2**: Understanding Cybersecurity Threats and the Need for AI
- **Topic 3**: Introduction to AI-Powered Cyber Defense Systems
- **Topic 4**: Tools for AI in Cybersecurity: Overview of Major Platforms
- **Topic 5**: Implementing AI for Threat Detection in Network Security
- **Topic 6**: Real-Time Detection and Automation with AI
- **Reflection & Review**: Reviewing the day's lessons through group discussion and a quick practical demo.

Day 2: Advanced Techniques in AI for Cyber Defense

- **Topic 1**: Machine Learning for Malware Detection
- **Topic 2**: Predictive Analytics in AI for Cybersecurity
- **Topic 3**: Autonomous Defense Systems Powered by AI
- **Topic 4**: Adversarial AI: Techniques to Detect and Prevent Attacks
- **Topic 5**: Cyber Threat Simulation and AI Response
- **Topic 6**: Evaluating AI Tools for Threat Mitigation in Real-Time
- **Reflection & Review**: Interactive session with scenario analysis and live tool use.

AGILE LEADERS
Training Center

Day 3: Securing AI Systems and Implementing Safeguards

- **Topic 1**: Security Challenges in AI Systems
- **Topic 2**: Securing Machine Learning Models Against Attacks
- **Topic 3**: Verification and Validation of AI-based Security Systems
- **Topic 4**: Ethical Considerations in AI for Cybersecurity
- **Topic 5**: Privacy Concerns and AI-driven Cyber Defense
- **Topic 6**: Creating Robust AI Systems for Cybersecurity
- **Reflection & Review**: Group discussion and assessment of challenges faced in securing AI systems.

Day 4: Implementing AI in Incident Response and Automation

- **Topic 1**: Automation of Cybersecurity Tasks Using AI
- **Topic 2**: AI in Incident Response and Data Breach Detection
- **Topic 3**: Using AI for Phishing Detection and Prevention
- **Topic 4**: Real-time Threat Analysis with AI Tools
- **Topic 5**: Integrating AI in SIEM Systems
- **Topic 6**: Future Trends in AI-Driven Cybersecurity
- **Reflection & Review**: Evaluating real-world examples of AI in cybersecurity response.

Day 5: Hands-On Workshops and Application in Real-World Scenarios

- **Topic 1**: Hands-on: Setting up AI for Network Intrusion Detection
- **Topic 2**: Workshop on Developing a Machine Learning Model for Threat Prediction
- **Topic 3**: AI-based Tools for Risk Assessment and Vulnerability Scanning
- **Topic 4**: Creating a Cyber Defense Strategy Using AI Models
- **Topic 5**: Preparing for Cybersecurity Challenges with AI Integration
- **Topic 6**: Implementing End-to-End Security with AI-Driven Tools
- **Reflection & Review**: Final discussion and feedback on the training.

AGILE LEADERS
Training Center

FAQ:

What specific qualifications or prerequisites are needed for participants before enrolling in the course?

Participants should have a basic understanding of cybersecurity principles and experience working in IT security roles. Familiarity with network security concepts and basic machine learning concepts would be beneficial but not mandatory.

How long is each day's session, and is there a total number of hours required for the entire course?

Each day's session is generally structured to last around 4-5 hours, with breaks and interactive activities included. The total course duration spans one week, approximately 20-25 hours of instruction.

How does AI enhance cybersecurity, and what challenges should organizations consider before implementing AI-driven solutions?

AI enhances cybersecurity by automating threat detection, improving decision-making, and predicting vulnerabilities before they materialize. However, organizations should be mindful of challenges such as ensuring the security of AI models, managing data privacy, and addressing potential adversarial AI attacks

How This Course is Different from Other AI in Cybersecurity Courses:

Unlike other courses that focus solely on theoretical knowledge, this course integrates hands-on workshops, real-world simulations, and practical tools, making it easier for participants to implement AI in their day-to-day cybersecurity practices. By focusing on both the security of AI systems and their application in real-world scenarios, this course stands out by addressing both the technical and ethical aspects of AI in cybersecurity. Participants will gain actionable skills that will directly impact their ability to protect networks and systems against evolving cyber threats.