AI in Cybersecurity: Predictive Threat Detection

Duration: 5 Days

Language: en

Course Code: PI2 - 118

Objective

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

- Understand how AI and machine learning are used in cybersecurity.
- Identify patterns and anomalies that signal cyber threats using AI tools.
- Implement AI-driven intrusion detection and behavior analysis.
- Explore autonomous defense mechanisms and automated incident response.
- Evaluate AI solutions for threat prediction and real-time protection.
- Address privacy, bias, and accountability in AI security systems.
- Design a roadmap for integrating AI into cybersecurity frameworks.

Audience

This course is ideal for:

- Cybersecurity analysts and IT security professionals.
- Security operations center (SOC) team members.
- Network and infrastructure engineers.
- AI and machine learning engineers working in security.
- CISOs, CTOs, and technology risk leaders.
- Ethical hackers and penetration testers.
- Government and military cybersecurity units.

Training Methodology

The course blends theoretical frameworks with technical demonstrations, scenario-based exercises, and tool walkthroughs. Participants will explore current AI security platforms, analyze attack simulations, and design AI-enhanced defense protocols. Group activities focus on risk evaluation and ethical implementation.

Summary

As cyber threats become more complex and frequent, traditional security tools alone are no longer sufficient. Artificial Intelligence (AI) is now playing a critical role in transforming cybersecurity from reactive protection to proactive defense. By using machine learning and automation, AI systems can detect anomalies, predict attacks, and even respond to threats autonomously in real time.

This course offers a practical exploration of how AI is integrated into modern cybersecurity operations. Participants will learn about AI-powered threat detection, behavioral analytics, autonomous response systems, and the ethical considerations of handing over decisions to intelligent machines. Through real-world examples and hands-on simulations, learners will gain the skills needed to enhance digital defenses with AI technologies.

Course Content & Outline

Section 1: The Role of AI in Modern Cybersecurity

- Cybersecurity challenges in a hyperconnected world.
- Limitations of traditional threat detection systems.
- Introduction to AI and machine learning in security.
- Key technologies: supervised vs. unsupervised learning, anomaly detection.
- Cyber threat landscape: phishing, ransomware, zero-day exploits.
- Case study: How AI stopped a real-world cyberattack.

Section 2: Predictive Threat Detection with AI

- Behavioral analysis and user activity modeling.
- Machine learning for threat hunting and anomaly spotting.
- AI in email security, fraud detection, and phishing prevention.
- Natural Language Processing (NLP) in analyzing malicious communication.
- Building datasets and training security models.
- Hands-on demo: AI-based threat prediction in SIEM systems.

Section 3: Autonomous Response and Real-Time Defense

- What is autonomous defense? From alert to action.
- SOAR (Security Orchestration, Automation, and Response) platforms.
- Automated patching, isolation, and mitigation techniques.

- AI-powered endpoint protection and network firewalls.
- Incident response bots and playbooks.
- Simulation: Responding to a breach using AI automation.

Section 4: Challenges, Risks, and Ethical Considerations

- Risks of false positives/negatives and automation errors.
- Bias in security models and fairness in AI responses.
- Balancing speed with human oversight.
- Privacy and legal implications in AI-driven surveillance.
- Transparency and explainability in AI decisions.
- Governance models for responsible AI in cybersecurity.

Section 5: Implementing AI in Cyber Defense Strategy

- Integrating AI tools into existing cybersecurity infrastructure.
- Choosing the right platforms and vendors.
- Skills and team requirements for AI-enhanced operations.
- Building cross-functional collaboration between AI and security teams.
- Metrics for success: detection rate, response time, incident reduction.
- Roadmap: Designing your AI-in-cybersecurity action plan.

Certificate Description

Upon successful completion of this training course, delegates will be awarded a Holistique Training Certificate of Completion. For those who attend and complete the online training course, a Holistique Training e-Certificate will be provided.

Holistique Training Certificates are accredited by The CPD Certification Service (CPD), and are certified under ISO 9001 and ISO 29993 standards.

CPD credits for this course are granted by our Certificates and will be reflected on the Holistique Training Certificate of Completion. In accordance with the standards of The CPD Certification Service, one CPD credit is awarded per hour of course attendance. A maximum of 50 CPD credits can be claimed for any single course we currently offer.

Categories

AI, Data and Visualisation, Technology

Tags

Artificial Intelligence, Threats, AI in Cybersecurity

Related Articles

The Importance of Cyber Security Training in Today's World

Discover why cybersecurity training is critical in today's digital world. Learn about threats, training benefits, legal compliance, and risk reduction for organisations.