KOENIG SOLUTIONS · COURSE OUTLINE

AI Cybersecurity: Threat Detection & SOAR

Learn to apply AI for threat detection, anomaly monitoring, and SOAR-driven incident response in cybersecurity operations.

5 Days	5	71
40 HOURS	MODULES	TOPICS

COURSE OVERVIEW

This course covers the role of artificial intelligence in cybersecurity, including its evolution, benefits, challenges, and applications such as intrusion detection, SIEM, and identity and access management. It then examines AI-powered threat detection and prevention, covering attack vectors, machine learning and deep learning techniques, vulnerability management, malware analysis, and threat intelligence. It moves on to anomaly detection and behaviour monitoring across networks, endpoints, insider threats, fraud, and deception technologies. Finally, it addresses AI-driven incident response and SOAR platforms, digital forensics, ethical and regulatory considerations, adversarial attacks, and future trends and industry use cases.

WHO THIS COURSE IS FOR

SOC Analysts | **Security Engineers** | **Threat Intelligence Analysts** | **Incident Responders** | **Cybersecurity Managers** | **Fraud Analysts**

LEARNING OBJECTIVES

- Explain the role of AI and machine learning in cybersecurity
- Identify cyber threats and attack vectors including APTs and malware
- Apply AI techniques for threat detection and phishing prevention
- Analyse network and endpoint data for anomaly and behaviour monitoring
- Assess insider threats and fraud using behavioural analytics
- Implement SOAR platforms and AI-driven playbooks for incident response
- Evaluate ethical, bias, and regulatory issues in AI cybersecurity
- Compare adversarial attack techniques and AI robustness defenses

COURSE SYLLABUS

5 Modules, 71 Topics

01

Introduction to AI in Cybersecurity

UNDERSTANDING ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

- Definition and Types of AI (Machine Learning, Deep Learning, NLP)
- Differences Between AI, ML, and Traditional Security Approaches
- Role of AI in Modern Cybersecurity

EVOLUTION OF AI IN CYBERSECURITY

- Historical Perspective of AI in Cyber Defense
- Key Milestones in AI-Driven Security
- Current Trends and Future Growth

BENEFITS AND CHALLENGES OF AI IN SECURITY OPERATIONS

- Advantages of AI in Threat Detection and Response
- Limitations of AI in Cybersecurity
- Ethical Concerns and Bias in AI Algorithms

APPLICATIONS OF AI IN CYBERSECURITY

- AI in Intrusion Detection and Prevention Systems (IDPS)
- AI-Powered Security Information and Event Management (SIEM)
- AI in Identity and Access Management (IAM)

02

AI-Powered Threat Detection and Prevention

UNDERSTANDING CYBER THREATS AND ATTACK VECTORS

- Types of Cyber Threats (Malware, Phishing, Ransomware, APTs)
- Attack Lifecycle and Kill Chain Analysis
- Role of AI in Detecting Advanced Persistent Threats (APTs)

AI TECHNIQUES FOR THREAT DETECTION

- Supervised vs. Unsupervised Machine Learning for Threat Detection
- Deep Learning and Neural Networks in Cybersecurity
- AI for Email Security and Phishing Detection

AUTOMATED VULNERABILITY SCANNING AND PATCH MANAGEMENT

- AI-Based Vulnerability Management Solutions
- Predictive Analysis for Patch Prioritization
- Role of AI in Zero-Day Threat Mitigation

AI IN MALWARE ANALYSIS AND CLASSIFICATION

- Traditional vs. AI-Based Malware Detection
- AI Techniques for Identifying Polymorphic Malware
- Machine Learning Models for Malware Classification

AI-POWERED THREAT INTELLIGENCE AND CYBERSECURITY ANALYTICS

- AI in Threat Intelligence Platforms (TIPs)
- Big Data Analytics and AI in Security Monitoring
- AI-Driven Threat Attribution and Response

03

AI for Anomaly Detection and Behaviour Monitoring

INTRODUCTION TO ANOMALY DETECTION IN CYBERSECURITY

- Defining Anomalies and Their Impact on Cybersecurity
- AI-Based Approaches for Anomaly Detection
- Challenges in AI-Powered Anomaly Detection

AI MODELS FOR NETWORK AND ENDPOINT MONITORING

- AI in Network Intrusion Detection Systems (NIDS)
- AI for Endpoint Detection and Response (EDR)
- Behavioral Profiling for Endpoint Security

BEHAVIORAL ANALYTICS FOR INSIDER THREAT DETECTION

- Identifying Anomalous User Behaviors
- AI in Monitoring Employee Activity and Preventing Data Breaches
- Case Studies of AI-Driven Insider Threat Detection

AI IN FRAUD DETECTION AND IDENTITY MANAGEMENT

- AI for User Authentication and Behavioral Biometrics
- Fraud Detection Using AI in Financial Transactions
- AI-Enabled Risk-Based Access Control (RBAC)

AI AND DECEPTION TECHNOLOGIES FOR CYBER DEFENSE

- AI-Powered Honeypots and Deception Networks
- Using AI to Analyze Attacker Behavior in Decoy Environments
- AI in Proactive Cyber Defense Strategies

04

AI-Driven Incident Response and Security Automation

AI IN AUTOMATED INCIDENT DETECTION AND RESPONSE

- How AI Enhances Security Operations Center (SOC) Efficiency
- AI in Security Incident Correlation and Analysis
- Reducing False Positives with AI-Powered Threat Validation

SOAR (SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE) SOLUTIONS

- Overview of SOAR Platforms and Their Role in Security Automation
- AI-Driven Playbooks for Incident Response
- Automating Security Workflows with AI

AI IN DIGITAL FORENSICS AND THREAT HUNTING

- AI for Log Analysis and Anomaly Detection in Forensics
- Machine Learning for Threat Hunting and Indicators of Compromise (IoCs) Identification
- AI in Automating Threat Attribution

ETHICAL CONSIDERATIONS AND AI BIAS IN CYBERSECURITY

- Risks of AI-Generated False Positives and Negatives
- AI Bias and Fairness in Cybersecurity Decision-Making
- Regulatory Considerations and Compliance Challenges

LIMITATIONS AND PITFALLS OF AI IN CYBERSECURITY

- Adversarial AI and Attack Techniques Against AI Models
- Explainability and Transparency Issues in AI-Based Security
- **AI in Cybersecurity vs. Human Expertise:** Finding the Balance

05

Future of AI in Cybersecurity

EMERGING TRENDS IN AI AND CYBERSECURITY

- AI-Driven Autonomous Security Systems
- AI-Powered Cloud Security and Zero Trust Architecture
- Future Role of Generative AI in Cyber Defense

AI VS. ADVERSARIAL ATTACKS: RED-TEAMING AND DEFENSE MECHANISMS

- How Attackers Exploit AI Weaknesses
- Adversarial Machine Learning Attacks and Defenses
- Techniques to Improve AI Robustness Against Cyber Threats

LEGAL, COMPLIANCE, AND REGULATORY ASPECTS OF AI IN CYBERSECURITY

- GDPR, CCPA, and AI Regulations in Cybersecurity
- AI in Compliance Audits and Risk Assessments
- Legal Responsibilities of AI-Powered Cybersecurity Solutions

INDUSTRY USE CASES AND BEST PRACTICES IN AI-POWERED CYBERSECURITY

- How Enterprises Are Implementing AI for Cyber Defense
- Best Practices for AI Model Training and Deployment in Security
- AI in Government and Critical Infrastructure Cybersecurity

FINAL TAKEAWAYS

- Recap of Key Learnings from the Training Program
- Open Discussion on Challenges in Implementing AI in Cybersecurity

WHAT IS INCLUDED

Everything You Need to Succeed

- Koenig course material for every module
- Delivery by certified instructors and subject matter experts
- Hands-on exercises throughout the course
- Course completion certificate from Koenig

ABOUT KOENIG

Who We Are

Established in 1993, Koenig Solutions is a globally recognised training provider with 35+ technology partnerships, 5,000+ training programmes and a network of certified instructors and subject matter experts, supporting individuals and enterprise teams worldwide.

FLEXIBLE DELIVERY

Learn the Way That Suits You

Classroom Training | Live Online Classes (ILO) | Fly-Me-A-Trainer (FMAT) | Flexi (Self-Paced) | 1-on-1 Training

Ready to Get Started?

Talk to a learning advisor about schedules, group training and customised delivery.

Visit koenig-solutions.com | info@koenig-solutions.com