AI in Cybersecurity

Duration: 5 Days (40hrs)

1: Introduction to AI in Cybersecurity

1.1 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

1.2 Evolution of AI in Cybersecurity

Historical Perspective of AI in Cyber Defense

Key Milestones in AI-Driven Security

Current Trends and Future Growth

1.3 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

1.4 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)

2: AI-Powered Threat Detection and Prevention

2.1 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)

2.2 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

2.3 Automated Vulnerability Scanning and Patch Management

AI-Based Vulnerability Management Solutions

Predictive Analysis for Patch Prioritization

Role of AI in Zero-Day Threat Mitigation

2.4 AI in Malware Analysis and Classification

Traditional vs. AI-Based Malware Detection

AI Techniques for Identifying Polymorphic Malware

Machine Learning Models for Malware Classification

2.5 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

3: AI for Anomaly Detection and Behaviour Monitoring

3.1 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

3.2 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

3.3 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

3.4 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)

3.5 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

4: AI-Driven Incident Response and Security Automation

4.1 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

4.2 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

4.3 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

4.4 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

4.5 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

5: Future of AI in Cybersecurity

5.1 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

5.2 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

5.3 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

5.4 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

5.5 Final Takeaways

Recap of Key Learnings from the Training Program

Open Discussion on Challenges in Implementing AI in Cybersecurity

Q&A