Datastat Research
Building Capacity in Training and Research

DATASTAT TRAINING IN

OFFICIAL COURSE PROSPECTUS

Center for Advanced Research & Professional Development

Nairobi Training Center • Global Virtual Academy • Corporate On-Site

ARTIFICIAL INTELLIGENCE AND BLOCK CHAIN

Adversarial AI and Model Attacks Training Course

Comprehensive Course Syllabus, Practical Modules & Upcoming Schedules

PROGRAM SPECIFICATIONS & HIGHLIGHTS

DURATION
5 Days Practical Hands-on

DELIVERY MODES
In-Person Class & Live Virtual

CERTIFICATION
Accredited Certificate of Completion

INTAKES / DATES
Multiple Cohort Schedules Included

PREPARED FOR:

Valued Participant

Email: training@datastatresearch.org | Issued: November 22, 2026

Academic & Professional Training Year: 2026

DATASTAT TRAINING INSTITUTE

P.O. Box 102802-00101, Nairobi, Kenya

Training Centers: Nairobi • Mombasa • Kigali • Dubai • Live Virtual Academy

Tel: +254 724 527 104 | +254 734 969 612

Email: training@datastatresearch.org

www.datastatresearch.org

Adversarial AI and Model Attacks Training Course

Artificial Intelligence And Block Chain • 5 Days Intensive • Accredited Certification

Course Overview

Adversarial AI and Model Attacks Training Course provides a comprehensive exploration of AI security, machine learning robustness, adversarial machine learning, model vulnerability assessment, and secure AI engineering.

Key Skills & Software Tools Covered

Adversarial AI • Model attack detection • AI security • Adversarial robustness

Upcoming Training Schedules

Confirmed cohort intakes and venues. Both physical in-person classroom and live virtual online seats are available.

TRAINING DATES	LOCATION / VENUE	FORMAT / DURATION	INVESTMENT (FEE)
21 Sep 2026 – 25 Sep 2026	Nairobi	Classroom / 5d	**$1,500 USD / KES 110,000**
21 Sep 2026 – 25 Sep 2026	Kigali	Classroom / 5d	**$3,000 USD / KES 110,000**
21 Sep 2026 – 25 Sep 2026	Dubai	Classroom / 5d	**$5,000 USD / KES 110,000**
21 Sep 2026 – 25 Sep 2026	Cape Town	Classroom / 5d	**$4,500 USD / KES 110,000**
21 Sep 2026 – 25 Sep 2026	Addis Ababa	Classroom / 5d	**$3,000 USD / KES 110,000**
21 Sep 2026 – 25 Sep 2026	Singapore	Classroom / 5d	**$5,000 USD / KES 110,000**
21 Sep 2026 – 25 Sep 2026	Istanbul	Classroom / 5d	**$5,000 USD / KES 110,000**
21 Sep 2026 – 25 Sep 2026	Bangkok	Classroom / 5d	**$5,000 USD / KES 110,000**
21 Sep 2026 – 25 Sep 2026	Accra	Classroom / 5d	**$4,000 USD / KES 110,000**
28 Sep 2026 – 2 Oct 2026	Nairobi	Classroom / 5d	**$1,500 USD / KES 110,000**
28 Sep 2026 – 2 Oct 2026	Kigali	Classroom / 5d	**$3,000 USD / KES 110,000**
28 Sep 2026 – 2 Oct 2026	Dubai	Classroom / 5d	**$5,000 USD / KES 110,000**

* Corporate discounts and customized cohort scheduling are available for teams of 3 or more participants.

Course Curriculum & Modules

Adversarial AI and Model Attacks Training Course

Introduction

Adversarial AI and Model Attacks Training Course provides a comprehensive exploration of AI security, machine learning robustness, adversarial machine learning, model vulnerability assessment, and secure AI engineering. As artificial intelligence systems become central to cybersecurity, healthcare, finance, autonomous systems, and enterprise decision-making, attackers are developing sophisticated techniques to manipulate, exploit, and compromise AI models. This course equips professionals with advanced knowledge of adversarial attacks, data poisoning, model evasion, prompt manipulation, AI threat intelligence, and defensive AI strategies to protect machine learning systems against emerging cyber threats.

Through hands-on learning, real-world case studies, and practical security exercises, participants will gain expertise in identifying weaknesses in AI pipelines, conducting adversarial testing, implementing model hardening techniques, and developing resilient AI solutions. The course focuses on AI risk management, trustworthy AI, machine learning security, secure model deployment, AI governance, and next-generation cyber defense frameworks, enabling organizations to build reliable and attack-resistant artificial intelligence ecosystems.

Course Duration

5 Days

Course Objectives

- Understand adversarial artificial intelligence concepts, attack surfaces, and AI security fundamentals.
- Identify and analyze machine learning model vulnerabilities and security weaknesses.
- Perform adversarial testing and AI penetration testing methodologies.
- Apply techniques for detecting and mitigating adversarial examples and model manipulation attacks.
- Understand data poisoning, backdoor attacks, and training data security risks.
- Implement robust machine learning and adversarial defense mechanisms.
- Conduct AI threat modeling and risk assessment for machine learning systems.
- Analyze model extraction, inversion attacks, and intellectual property risks.
- Secure large language models (LLMs) and generative AI systems against attacks.
- Apply AI red teaming and security validation frameworks.
- Develop strategies for secure AI lifecycle management and model governance.
- Use modern tools for AI vulnerability discovery and adversarial simulation.
- Build resilient AI systems aligned with responsible AI, cybersecurity, and trust principles.

Target Audience

- AI and Machine Learning Engineers
- Cybersecurity Professionals and Security Analysts
- Penetration Testers and Ethical Hackers
- Data Scientists and ML Researchers
- Security Architects and Cloud Security Engineers
- AI Governance and Risk Management Professionals
- Software Developers Building AI Applications
- Technology Leaders and Digital Transformation Managers

Course Modules

Module 1: Foundations of Adversarial AI and AI Security

- Introduction to adversarial machine learning and AI threat landscapes
- Understanding AI attack surfaces and security challenges
- Machine learning lifecycle security risks
- AI trust, reliability, and robustness principles
- Overview of adversarial AI frameworks and standards
- Case Study: Autonomous Vehicle AI Manipulation: Analysis of how small environmental changes can influence computer vision models used in autonomous driving systems.

Module 2: Adversarial Examples and Evasion Attacks

- Understanding adversarial examples in deep learning models
- Image, audio, and text-based adversarial attacks
- Gradient-based attack methods
- Black-box and white-box attack techniques
- Detection and prevention of evasion attacks
- Case Study: Facial Recognition Evasion: Examination of techniques used to confuse facial recognition algorithms through adversarial inputs.

Module 3: Data Poisoning and Backdoor Attacks

- Training data manipulation techniques
- Data poisoning attack lifecycle
- Backdoor triggers in AI models
- Supply chain risks in AI datasets
- Data validation and protection strategies
- Case Study: Compromised AI Training Dataset: Investigation of how poisoned datasets can create hidden vulnerabilities in deployed models.

Module 4: Model Extraction and Privacy Attacks

- Model stealing and intellectual property threats

- Query-based model extraction attacks
- Membership inference attacks
- Model inversion techniques
- Privacy-preserving machine learning defenses
- Case Study: Commercial AI Model Theft: Analysis of risks when attackers replicate proprietary machine learning models through API interactions.

Module 5: Large Language Model (LLM) Attacks and Generative AI Security

- LLM vulnerabilities and attack techniques
- Prompt injection and jailbreak attacks
- Retrieval-augmented generation (RAG) security risks
- AI agent manipulation threats
- Securing generative AI applications
- Case Study: Enterprise Chatbot Security Breach: Assessment of how malicious prompts can manipulate AI assistants and expose sensitive information.

Module 6: Adversarial AI Testing and Red Teaming

- AI security testing methodologies
- Machine learning penetration testing approaches
- AI red team operations
- Attack simulation frameworks
- Vulnerability reporting and remediation
- Case Study: Financial Fraud Detection Model Testing: Conducting adversarial testing against an AI-powered fraud detection system.

Module 7: Defensive AI Engineering and Model Hardening

- Robust model training techniques
- Adversarial training approaches
- Secure AI deployment practices
- Model monitoring and anomaly detection
- Continuous AI security improvement
- Case Study: Healthcare AI Protection: Hardening diagnostic AI systems against adversarial manipulation.

Module 8: AI Governance, Risk Management, and Future Threats

- AI security governance frameworks
- Responsible AI and trustworthy AI principles
- AI risk assessment methodologies
- Regulatory considerations for secure AI
- Future trends in adversarial AI attacks
- Case Study: Enterprise AI Governance Program: Designing an AI security framework for organizations adopting large-scale AI systems.

Training Methodology

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@datastatresearch.org or call +254724527104

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to DATASTAT CONSULTANCY LTD account, as indicated in the invoice so as to enable us prepare better for you.

Certification & Learning Methodology

- Hands-on practical delivery with real-world datasets, case studies, and lab exercises.
- Post-training mentorship, access to class resources, and customized follow-up support.
- Participants who successfully complete the course receive an accredited Datastat Certificate of Completion.

How to Enroll & Reserve Your Seat

1. Online Registration: Visit https://datastatresearch.org/courses/adversarial-ai-and-model-attacks-training-course to register online.
2. Email Booking: Send participant details to training@datastatresearch.org for official invoice & reservation.
3. Support & Assistance: Inquire via phone +254 724 527 104 | +254 734 969 612.