Certified AI and LLM 'Bootcamp' in Addis Ababa

The objective of this course is to help cybersecurity professionals develop practical AI and Large Language Model (LLM) skills required to understand, secure, and operate AI-driven systems in modern environments. The course provides hands-on learning in AI fundamentals, LLM platforms, deep learning concepts, prompt engineering, AI risks, prompt injection attacks, API security, model behavior analysis, and secure AI deployment practices.

5 FULL DAYS | <DATE - TBD> | TRAINING FACILITIES AT <LOCATION>

- The course is designed to build AI literacy and practical cybersecurity skills for modern security teams.
- Focus on real-world AI security risks including prompt injection, exposed API keys, model abuse, bias, and adversarial prompting.
- Hands-on labs delivered through the CyCube platform with practical exercises and realistic scenarios.
- Includes exercises on CNN digit classification, LLM APIs, secure AI architectures, authentication, and model evaluation.
- Participants will gain confidence to assess AI systems, identify vulnerabilities, and integrate AI threat modeling into cybersecurity operations.
- Ideal for professionals seeking to strengthen their understanding of AI, LLM technologies, and associated security risks.
- **Course prerequisites:** Basic cybersecurity knowledge; familiarity with Windows and Linux systems; scripting experience with Python, PowerShell, or similar tools is recommended. Basic machine learning concepts are beneficial but not mandatory.

TARGET AUDIENCE

- Cybersecurity Professionals
- SOC Teams / Security Analysts
- Security Engineers
- Penetration Testers
- DevSecOps Engineers
- AI and Machine Learning Practitioners
- IT Security Managers
- Anyone interested in AI and LLM Security

THE INSTRUCTOR

Delivered by senior instructors with 10+ years of experience in cybersecurity and ICT systems, with strong hands-on and professional training expertise. Practical, scenario-based learning and hands-on labs are emphasized through realistic AI security exercises hosted on the CyCube platform.

ABOUT ECS ETHIOPIA

ECS Ethiopia is a technology-driven company working with government bodies, municipalities, and large corporations to bring advanced global solutions to Ethiopia. As part of the ECS Group (UK), we help finance and execute major projects while fostering strong partnerships and innovation across the country.

GLOBAL TRAINING PARTNERSHIPS

Our training programs and learning platform were developed in close collaboration with leading international training organisations. Thousands of professionals worldwide have successfully completed these programs using this training content and learning system.

ECS Ethiopia

MODULE 01
FOUNDATIONS OF AI AND LLMS
Understand the fundamentals of artificial intelligence, machine learning, and deep learning concepts used in cybersecurity. Learn how Large Language Models are built, trained, and exposed through APIs and platforms. Explore the role of generative AI in modern security operations and understand how attackers can abuse AI technologies.

MODULE 02
IMPLEMENTING LLM PLATFORMS SECURELY
Study different LLM deployment models including cloud-based, on-premises, and hybrid environments. Learn how to integrate AI services securely into applications and workflows. Understand authentication, authorization, logging, and isolation requirements necessary to operate AI systems securely.

MODULE 03
DIGIT CLASSIFICATION WITH CNNS
Explore the fundamentals of Convolutional Neural Networks and their building blocks. Learn how image classification models are trained, evaluated, and tested. Understand model limitations and relate CNN behavior to practical security applications such as malware detection and anomaly identification.

MODULE 04
PROMPTING AND SUMMARY ACCURACY
Examine effective prompting techniques and adversarial prompting concepts. Learn how to evaluate AI-generated summaries for accuracy, completeness, and hallucinations. Develop methods for validating AI-generated reports and building internal review processes.

MODULE 05
LLM BIAS: DETECTION AND EXPLANATION
Study the sources and types of bias that affect Large Language Models. Learn how biased outputs influence decision-making and security operations. Understand techniques to identify, explain, document, and mitigate bias in AI systems.

MODULE 06
PROMPT INJECTION IN AI CHAT APPLICATIONS
Understand common attack patterns targeting AI chat applications. Learn how prompt injection attacks are performed and how attackers manipulate model behavior. Study defensive techniques including input validation, system prompts, sandboxing, and policy controls.

MODULE 07
EXPOSED API KEYS IN AI NOTEBOOKS
Explore common AI development workflows and notebook environments. Learn how exposed API keys and secrets can be discovered and abused. Study secure development practices, secret management techniques, and methods to harden AI development environments.

MODULE 08
MODEL BEHAVIOR MAPPING VIA APIS
Learn how attackers and defenders systematically probe LLM APIs to understand model capabilities and limitations. Study behavior mapping techniques used to identify weaknesses, constraints, and jailbreak opportunities. Understand how these findings support red team exercises and defensive planning.

MODULE 09
AI ASSISTANT MISUSE VIA ROLE INJECTION
Examine the different roles used within AI systems and understand how role injection attacks manipulate model behavior. Learn how attackers bypass restrictions, override policies, and misuse AI assistants. Study guardrails, governance controls, and technical protections that reduce these risks.

MODULE 10
AI THREAT MODELING AND RISK MANAGEMENT
Develop the ability to incorporate AI and LLM-specific risks into existing cybersecurity frameworks. Learn how to identify attack surfaces, abuse scenarios, and trust boundaries within AI-enabled environments. Understand risk assessment methodologies and secure design principles for AI systems.

MODULE 11
SECURE AI DEVELOPMENT PRACTICES
Study secure coding principles, API security, secret management, and data handling requirements for AI applications. Learn best practices for protecting sensitive information and maintaining secure development lifecycles for AI-enabled solutions.

MODULE 12
AI SECURITY OPERATIONS AND DEFENSIVE STRATEGIES
Explore how AI technologies support cybersecurity operations and incident response activities. Learn methods for monitoring AI systems, identifying misuse, and implementing defensive controls. Understand how AI-specific security practices can be integrated into SOC operations and broader security programs.

HANDS-ON LABS
Course labs are delivered through the CyCube platform, a Software-as-a-Service (SaaS) environment designed to provide realistic, practical exercises without requiring local software installation. Participants will strengthen their skills, identify areas for improvement, and gain experience working with AI and LLM technologies in controlled scenarios.