Practical LLM Security: Attacks, RAG Exploitation, and Secure Design
(ความปลอดภัย LLM เชิงปฏิบัติ: การโจมตี ช่องโหว่ RAG และการออกแบบระบบอย่างปลอดภัย)

ระยะเวลาอบรม 2 วัน

หลักการและเหตุผล

หลักสูตรนี้มีวัตถุประสงค์เพื่อเสริมสร้างความรู้และทักษะด้านความมั่นคงปลอดภัยของระบบ LLM ในเชิงปฏิบัติ โดยครอบคลุมทั้งการวิเคราะห์ความเสี่ยงตาม OWASP Top 10 for LLM Applications การทดสอบและโจมตีระบบจริง และการออกแบบมาตรการป้องกัน เพื่อให้บุคลากรสามารถนำไปประยุกต์ใช้กับระบบ AI ในองค์กรได้อย่างมีประสิทธิภาพและปลอดภัย

วัตถุประสงค์

- เข้าใจ threat model ของ LLM systems
- สามารถทำ prompt injection / RAG attack ได้จริง
- สามารถออกแบบระบบ LLM แบบ secure-by-design
- เรียนรู้วิธี harden ระบบ (input / output / RAG)

รายละเอียดหลักสูตร

Day 1: Attack & Exploitation

- LLM Threat Modeling
- OWASP Top 10 for LLM
- Prompt Injection Deep Dive
- RAG Attack (Core Session)
- Data Exfiltration & Abuse
- Demo & Workshop: การทดสอบ Prompt Injection และ RAG Attack

Day 2: Defense & Secure Design

- Secure Design for LLM
- Prompt & Context Defense
- RAG Hardening
- Output Guardrails & Monitoring
- Demo & Workshop: Final Challenge: Secure an AI chatbot

หลักสูตรนี้เหมาะสำหรับ

- Developer / Backend / AI Engineer
- Security Engineer / AppSec / Red Team
- DevOps / Platform (ที่ดูแล AI system)

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th
Call us today 0-2634-7993-4
177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th