AI Security Awareness for Executives
(การตระหนักรู้ด้านความปลอดภัย AI สำหรับผู้บริหาร)

ระยะเวลาอบรม 1 วัน

หลักการและเหตุผล

หลักสูตรนี้ออกแบบมาเพื่อให้ผู้เริ่มต้นมีความเข้าใจพื้นฐานเกี่ยวกับความปลอดภัยในการประยุกต์ใช้งาน LLM/AI โดยนำเสนอถึงความเสี่ยงที่อาจเกิดขึ้นถ้าใช้งานอย่างขาดความระมัดระวังและตระหนักรู้ในการนำมาใช้งาน

วัตถุประสงค์

- เข้าใจความเสี่ยงของ LLM (ตาม OWASP Top 10 for LLM Applications)
- เห็นภาพ attack จริง เช่น prompt injection, RAG attack
- เข้าใจแนวทางป้องกันระดับ high-level
- สามารถนำข้อมูลไปใช้คุยกับทีมเพื่อออก requirement ได้

รายละเอียดหลักสูตร

- LLM & AI Risk Landscape
- OWASP Top 10 for LLM (Overview)
- Best Practices (High-level)
- Demo & Workshop: การทดสอบ Prompt Injection และ RAG Attack

สิ่งที่ผู้เรียนจะได้รับ

- ภาพรวมของความเสี่ยงในการใช้งาน LLM และ Generative AI อย่างขาดความระมัดระวัง
- อธิบายถึงความเสี่ยงแต่ละข้อใน OWASP Top 10 LLM แบบเข้าใจง่าย
- สาธิตความเสี่ยงและการโจมตีที่อาจเกิดขึ้น เช่น prompt injection, data leakage
- แนะนำแนวทางปฏิบัติที่ "ควรทำ" (ระดับ high-level ที่ยังไม่ลงรายละเอียดเชิงลึก) ในการนำ LLM และ Generative AI มาใช้งาน

หลักสูตรนี้เหมาะสำหรับ

- ผู้บริหารหรือผู้ที่เริ่มต้นสนใจการประยุกต์ใช้งาน LLM/AI ให้มีความมีปลอดภัย

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