CTR-810 AI Cyber

משך הקורס: 3 מפגשים – 24 שעות

אודות הקורס

קורס מעשי וממוקד שמסביר כיצד ניתן להשתמש בבינה מלאכותית בצורה אחראית ומאובטחת, גם ללא רקע טכני. הקורס מעניק כלים להבנה של סיכונים, שימוש בכלים ללא קוד (No-Code), ושמירה על אבטחת מידע.

נושאי הלימוד

מודול 1: מבוא לבינה מלאכותית ולסייבר

- מהי בינה מלאכותית – הסבר פשוט ודוגמאות
- מתי AI עלול "להמציא" תוצאות שגויות או מסוכנות
- מבוא לאיומי סייבר בעידן הבינה המלאכותית
- הקשר בין AI לסיכוני אבטחת מידע

מודול 2: כלים פופולריים של AI ללא קוד

- היכרות עם כלים כמו ChatGPT, Claude, Gemini, Canva AI ועוד
- כיצד מבצעים אינטגרציה פשוטה של AI בעסק או בפרויקט
- הסבר כללי על מה שקורה "מאחורי הקלעים" של הכלים האלו

מודול 3: מהם הסיכונים של שימוש לא מבוקר ב-AI

- סיכון לדליפת מידע רגיש
- תוצרים שגויים או מזיקים – איך מזהים אותם
- מתקפות Prompt Injection והשפעותיהן
- דוגמאות למתקפות מבוססות AI כמו התחזות, הנדסה חברתית ועוד

מודול 4: כיצד לבחון תוצרי AI לפני העלאה לפרודקשן

- כללים לבדיקה ידנית
- שימוש בכלים לבדיקת עובדות וסריקת תוכן
- בניית רשימת בדיקה לתוצריAI
- שמירה על תיעוד והיסטוריית החלטות

מודול 5: שמירה על פרטיות ומידע רגיש

- איך לזהות מידע שאסור להזין ל-AI
- ניהול הרשאות וגישה לכלים
- עבודה עם מודלים סגורים ומקומיים) כגוןOllama)
- היתרונות של הפעלת AI בסביבה מקומית

מודול 6: תרגול מעשי

- זיהוי תוצאה מזויפת שלAI
- שימוש בכלים פשוטים לבקרה
- תרגול יצירת נוהל שימוש בטוח ב-AI

מודול 7: יצירת מדיניות שימוש ארגונית

- כללי אצבע לשימוש בטוח עבור עובדים לא טכניים
- דוגמאות למסמכי מדיניות פשוטים וברורים
- יצירת נוהל לבדיקה, בקרה ואישור תכנים

מודול 8: סיכום ומשאבים להמשך

- מדריך לשימוש בטוח ב-AI
- המלצות לבחירת כלים
- משאבים להעמקה והמשך למידה