MLOps Essentials:
AI Lifecycle Management

<u>תיאור הקורס:</u>

לפתח מודל AI זה נחמד, אבל לגרום לו לעבוד בארגון לאורך זמן זה האתגר האמיתי.
קורס MLOps מלמד אתכם את הצד התפעולי של עולם ה AI .

נלמד איך לוקחים מודל חכם ומוודאים שהוא נשאר חכם, מאובטח ומעודכן בתוך אפליקציה חיה.
חשיבות הקורס נובעת מהצורך של חברות ב"שומרים "של הבינה המלאכותית - אנשים שיודעים לנהל את מחזור החיים של המודל.

למידת התחום משדרת מקצוענות וחדשנות ברמה הגבוהה ביותר.

<u>קהל יעד:</u>

אנשי תשתיות, מפתחים מתקדמים ואנשים שרוצים להתמחות בצד הניהולי-תפעולי של מהפכת הבינה המלאכותית.

סילבוס נושאים:

1.מבוא ל-MLOps: ממדע למוצר

- The MLOps Mindset: למה DevOps מסורתי לא מספיק למודלי AI?
- ההבדל בין סביבת מחקר (Notebooks) לסביבת ייצור (Production).
- סקירת מחזור החיים של מודל (Model Lifecycle) לפי הסטנדרטים המובילים בתעשייה.

2.ניהול נתונים וצינורות מידע (Data Pipelines)

- בניית Data Pipelines אוטומטיים להזנת המודל במידע טרי.
- איכות נתונים (Data Quality) ובדיקת תקינות המידע לפני כניסה למודל.
- הכרת מושגי יסוד בניהול גרסאות של דאטה (DVC).

3.פריסה ואוטומציה (CI/CD for ML)

- Automated Deployment: איך מעלים מודל לאוויר בצורה בטוחה.
- אסטרטגיות עדכון: החלפת מודלים ללא השבתת המערכת (Blue-Green / Canary Deployments).
- אריזה וקונטיינרים (Docker/Kubernetes) כבסיס להרצת AI בסביבות שונות.

4.ניטור ביצועים וזיהוי "זיופים" (Drift & Monitoring)

- Model Drift: למה מודלים מאבדים דיוק עם הזמן ואיך מזהים זאת בזמן אמת.
- הגדרת מדדי ביצוע (KPIs) טכניים ועסקיים למודל המבצע.
- מנגנוני התרעה (Alerting) ואימון מחדש אוטומטי (Retraining).

5.אבטחה והגנה על מודלים (AI Security)

- הגנה מפני התקפות הטיה (Adversarial Attacks) וגניבת מודלים.
- ניהול הרשאות וגישה לנתוני האימון ולתוצרי המודל.
- פרטיות במידע ושימוש ב-AI בסביבות רגולטוריות.

6.התייעלות וניהול משאבים (FinOps for AI)

- אופטימיזציה של משאבי מחשוב (GPU/CPU) להרצה זולה ויעילה.
- שימוש בטכניקות דחיסה וצמצום מודלים מבלי לפגוע בביצועים.
- מעקב עלויות ענן וניהול תקציב ה-AI הארגוני.

7.אתיקה, משילות ותחזוקה ארוכת טווח

- הטמעת כלי בדיקה לווידוא הוגנות (Fairness) ומניעת הטיות במודל.
- תיעוד מודלים (Model Cards) ושקיפות ארגונית.
- אסטרטגיות לשמירה על יציבות המערכת וניהול חוב טכני בעולם ה-AI.