הרצאה בנושא:

כשבינה מלאכותית הופכת לאויבת סמויה: סיכוני אבטחת מידע וסייבר במערכות מתקדמות

המועד	**27.01.2025 שעה: 14:00 עד 17:00**
מיקום	**מקוון Online**
מרצים	**אריק קליין** **אסי לב, COMMIT**
מחיר	**הרשמה מראש חובה!** **לחברי האיגוד: ללא עלות.** **לקהל הרחב: 300 ₪ (לפני מע"מ).** **ביטול השתתפות אחרי ה-25.01.2025 בתשלום מלא.**

סדר יום:

14:00-14:05	פתיחה - זיו אבטליון ואסף נבות, מובלי הקבוצה.
14:05-15:20	אריק קליין - כשבינה מלאכותית הופכת לאויבת סמויה: סיכוני אבטחת מידע וסייבר במערכות מתקדמות.
15:20-15:30	הפסקה
15:30-16:45	אסי לב - השפעת שילוב מרכיבי AI בתהליך הנדסת מערכות.
16:45-17:00	סיכום.

תקציר ההרצאה ראשונה:

כשבינה מלאכותית הופכת לאויבת סמויה: סיכוני אבטחת מידע וסייבר במערכות מתקדמות

העולם עובר מהפכה טכנולוגית, והבינה המלאכותית ניצבת בלב השינוי. אך לצד ההבטחה לשיפור תהליכים מורכבים ולשדרוג מערכות, מסתתרת סכנה: איך מתמודדים עם מערכות מבוססות AI שיכולות להפוך מכלי לייעול, לכלי בידי תוקף ערמומי?

בהרצאה זו נצלול אל עומקם של סיכוני אבטחת המידע והסייבר של מערכות מורכבות המשלבות בינה מלאכותית, המשלבות מודלי(LLM (Large Language Models רבי-עוצמה. נדון במתקפות ייחודיות כמו הרעלת נתונים, Adversarial attacks, ונציג אתגרי אבטחת המידע קלאסיים בהם מידע רגיש, ערכי וקניין רוחני יזלגו מתוך הארגון.

ההרצאה תספק למשתתפים כלים מעשיים להתמודדות עם איומים אלו, לצד מחשבה מעמיקה על אתיקה, אמינות ואחריות במערכות מבוססות AI. בואו לגלות איך לשמור על מערכות העתיד שלכם חכמות - אך גם מוגנות.

על המרצה:

אריק קליין הוא מומחה לייעוץ אסטרטגי בניהול סיכוני סייבר בטכנולוגיות מתקדמות, עם למעלה מ-30 שנות ניסיון בניהול בכיר ולמעלה מעשור של התמחות בתחום הסייבר. הוא מתמקד במתן פתרונות סייבר לשילוב טכנולוגיות חדשניות בארגוניים, ובתוך כך שירותי ענן, בינה מלאכותית ואבטחת שרשרת האספקה. אריק מביא עמו ניסיון רב בהגדרה ויישום של מדיניות סייבר, מודלים לניתוח סיכונים, הנחיות טכנולוגיות ותהליכי עבודה עבור מגוון רחב של ארגונים ציבוריים.

הרצאה בנושא:

כשבינה מלאכותית הופכת לאויבת סמויה: סיכוני אבטחת מידע וסייבר במערכות מתקדמות

המועד	**27.01.2025 שעה: 14:00 עד 17:00**
מיקום	**מקוון Online**
מרצים	**אריק קליין** **אסי לב, COMMIT**
מחיר	**הרשמה מראש חובה!** **לחברי האיגוד: ללא עלות.** **לקהל הרחב: 300 ₪ (לפני מע"מ).** **ביטול השתתפות אחרי ה-25.01.2025 בתשלום מלא.**

בנוסף, הוא מתמחה בניהול סיכוני משפט וסייבר של מערכות מבוססות בינה מלאכותית. הוא פיתח מודל מקיף להערכת סיכונים ומתודולוגיית צמצום, המבוססים על רגולציות גלובליות ו- Best practices בתעשייה.

תקציר ההרצאה שניה:

השפעת שילוב מרכיבי AI בתהליך הנדסת מערכות

ההרצאה תספק למשתתפים הבנה של האתגרים וההזדמנויות בשילוב AI בתהליך הנדסת מערכות, ותציג גישות וכלים להתמודדות עם מורכבויות אלו.

בהרצאה נעסוק בהשפעת שילוב מרכיבי בינה מלאכותית (AI) בתהליך הנדסת מערכות, תוך התמקדות בזיהוי הצורך ב AI-באיסוף הדרישות הפונקציונליות של המערכת. נדון בהערכת בשלות הארגון לשילוב AI, כולל היבטי תשתיות מחשוב, אחסון ותקשורת המותאמים לפרויקטי AI וכן נבחן את מוכנות הנתונים בארגון, בהתייחס למבנה, איכות, נפח, ומגבלות פרטיות ורגולציה.

בנוסף, נדון באילוצי אבטחת מידע והגנת המידע בשימוש ב AI-, בהגדרת שאלות מחקר, ובהתאמת המידע לצורך שימוש במודלי AI. יוצגו תהליכי הערכה ומדידת הצלחה של מודלים, והשיקולים בהחלטה בין אימון מודל חדש לבין שימוש במודל מאומן מראש. כמו כן, נבחן את הזמן המתאים לשילוב פלטפורמת MLOps בתהליך הפיתוח, ואת השיקולים בבחירת מודלים ושיטות אירוח.

ההרצאה תספק כלים ושיטות לשיפור והתאמת מודלים לצרכים ייחודיים, ומעקב אחר שינויים בביצועי הAI-נדון בהגנה מפני סיכונים הנובעים משימוש ב AI-, בפיתוח באמצעות מסגרות עבודה (Frameworks)ל AI-, ובתכנון ארכיטקטורות למערכות משולבות AI. יוצגו גישות לאבטחת איכות, כולל כיצד ומה לבדוק במערכות משולבות AI, ואילו מדדים להשתמש להערכת הביצועים.

לבסוף, אם יותיר לנו הזמן נדון בתחזוקת המערכת, כולל ניטור ופיקוח על סטיות במודלי AI, איכות הנתונים, שימוש במודל, ומשמעויות כלכליות.

על המרצה:

הרצאה בנושא:

כשבינה מלאכותית הופכת לאויבת סמויה: סיכוני אבטחת מידע וסייבר במערכות מתקדמות

המועד	**27.01.2025 שעה: 14:00 עד 17:00**
מיקום	**מקוון Online**
מרצים	**אריק קליין** **אסי לב, COMMIT**
מחיר	**הרשמה מראש חובה!** **לחברי האיגוד: ללא עלות.** **לקהל הרחב: 300 ₪ (לפני מע"מ).** **ביטול השתתפות אחרי ה-25.01.2025 בתשלום מלא.**

אסי לב, הינו ה CTO-של חטיבת ה ICT-בחברתCommit ומביא עמו ניסיון של מעל 20 שנים בפיתוח תוכנה, עם מומחיות במחקר והנדסת מערכות בתחום ה-Machine Learning. אסי פיתח מערכות מורכבות ורב-תחומיות המשלבות בינה מלאכותית ולו ניסיון רב בהנדסת תשתיות טכנולוגיות בתחומי התקשורת, אבטחת מידע, מערכות הפעלה וענן .

כחלק מתפקידו של אסי כ CTO , אסי מוביל \ בחינת והטמעת טכנולוגיות חדשות, בניית הוכחות יכולת (POC) חדשניות והובלת פרויקטים רב-תחומיים, במיוחד בתחומי לימוד מכונה, בינה מלאכותית וGenerative AIi . קודם לכך אסי, שימש כ- Chief Architect בקבוצת Commit והיה אחראי על טכנולוגיות וארכיטקטורות של פרויקטים חוצי ארגון, כולל בניית ארכיטקטורות מבוססות מיקרו-שירותים תוך התמקדות בתפעול, ניטור, אבטחת מידע וביצועים.

לחץ/לחצי כאן למעבר לזימון באתר.

לחץ/לחצי כאן למעבר הרשמה מקוונת ישירה.

לחץ/לחצי כאן לזימון בפורמט PDF.