חשיפת מידע רגיש במערכות GenAI

בשנים האחרונות מתעצם השימוש מערכות בינה מלאכותית הן בחיינו האישיים והן באלו המקצועיים. השימוש במערכות AI טומן בחובו יתרונות רבים כמו הגברת הפרודוקטיביות, ייעול זמנים ותהליכים, עידוד חדשנות וצמיחה, שיפור הדיוק והפחתת טעויות אנוש. עם זאת, כלי AI כמו ChatGPT ו-Copilot עשויים לאסוף כמויות גדולות של מידע רגיש, מה שמעלה חששות לגבי דלף מידע רגיש ביטחונית ומסווג עסקית וכן לגבי פרטיות המשתמשים.

מערכות ה - AI פועלת, בין השאר, בשיטת צבר מידע ולמידה מאינטראקציות עם המשתמשים. כלל המידע שאנו מזינים ומעבדים נשמר ומוצלב עם המידע הקיים, ולכן גם המידע הבלתי מסווג שאנו מזינים עלול לחשוף נתונים רגישים. בנוסף לכך, התוצר מתהליכי השימוש במערכות AI עלול להיות מנוצל על ידי תוקפים שמטרתם לשבש אותו, לפגוע באמינותו או בזמינותו (לדוגמה, חדירה או פגיעה בתהליכי פיתוח קוד).

דגשים מרכזיים לשימוש בטוח:

- בלמ"ס בלבד - אין להזין / לעבד מידע חסוי, רגיש או מסווג במערכות GenAI
- השימוש במערכת יתבצע באמצעות התשתית המאושרת והמוגנת של החברה (בחלקה היא תשתית Enterprise אלביטאית, שמטרתה לצמצם סיכונים ולהבטיח שמירה על מידע).
- אין לחשוף קניין רוחני או חומר מוגן בזכויות יוצרים ללא אישור.
- אין לשתף מידע על לקוחות, פרויקטים, תוכניות עסקיות או מידע טכנולוגי (אם במסגרת השימוש צפוי להיחשף מידע כזה, יש לגבש עקרונות ביטחון מראש עם ממונה הביטחון של היחידה העסקית).
- שיתוף קוד תוכנה, במיוחד כזה שפותח עבור צה"ל, דורש זהירות רבה בשל רגישותו וחשיבותו הייחודית.
- הימנעו מהזנת מידע אישי של עובדים.

זכרו: גם AI עלולה לטעות. היו זהירים, מודעים למידע שאתם חושפים, לבדיקות שנדרש לבצע לתוצרים בכל הקשור להכללתם במערכות, תשתיות, מוצרי ותהליכי העבודה בחברה.

אלביט מערכות
מטה החברה • ביטחון

Elbit Systems
ESOC