# הלב והמוח של מלחמת הסייבר הבאה

למידת מכונה (ML), אחד מהיישומים הנפוצים של בינה מלאכותית, מאתגרת את עולם הסייבר בהיותה טכנולוגיה חדשה ומתפתחת. הטמעתה מעלה שאלות כמו כיצד מטמיעים אותה בתשתית האבטחה, כיצד מורידים את הסיכון והאם יש צורך לגייס לצורך פרויקט כזה מדעני נתונים? | **צופית שחר**

בינה מלאכותית (AI) היא מונח רחב מאוד המתייחס לכל מה שקשור ל"מחשב-ללא-אדם", אולם יש היבט אחד של AI אשר צובר תאוצה משמעותית והוא היכולת להעצים מערכות על מנת שיבצעו משימות, שמתאימות יותר למכונות מאשר לבני אדם. משימות אלה מאופיינות בכמויות מאסיביות של נתונים, מגוון גדול של נתונים ובצורך לעבד במהירות את הנתונים הללו בעזרת זיהוי דפוסים. זה בדיוק המקום בו למידת מכונה (ML), אחד מהיישומים הנפוצים של AI, נכנסת לעולם הסייבר ככלי מקצועי.

בדוח חדש של SBIC (Security for Business Innovation Council) נשאלו Ciso מארגונים מובילים בעולם, מה הם התחומים המרכזיים בהם מנהלי אבטחה צריכים להתמקד בתהליך של יישום ML ו-AI בארגונם. השאלות שעלו הן כיצד מתחילים בהטמעה של ML בתשתית האבטחה, כיצד מורידים את הסיכון כשמתמודדים עם טכנולוגיה חדשה כמו ML, האם יש צורך לגייס לצורך פרויקט כזה מדעני נתונים ובכלל - מה הם הצעדים ליישום ML. להלן כמה תובנות עיקריות העולות מדוח SBIC.

## צעד אחד קדימה

פיתוח של למידת מכונה והטמעת שפת מכונה, הם רלוונטיים מאוד בפעולות הגנת המידע והסייבר, אם כי זה מצריך לא מעט הכנות וחשיבה אסטרטגית נכונה. הצעד הראשון, עליו ממליצים מנהלי הגנת הסייבר אשר השיבו לסקר, כי חייב להיות זיהוי הבעיה, ולאחר מכן צריך להבין אם הטכניקות של למידת מכונה אכן יתמכו בדרך לפתרון. אם כן, יהיה צורך בכמויות עצומות של נתונים, בתצורה הניתנת לעיבוד עבור האלגוריתם העתידי שעתיד לזהות דפוסים כאלה ואחרים. לכן, בנייה עצמית של פתרון למידת מכונה דורש יכולת לבחור את הנתונים "הנקיים ביותר", ואז לבצע בחינות חוזרות ונשנות של

**צופית שחר** | צילום: הדר שחר

האלגוריתם ותהליך קבלת ההחלטות שלו בסביבה חיה. כמו כל עולם הסייבר, למידת מכונה זה משהו שנמצא בתהליך מתמשך ותמידי.

אולם למידת מכונה בעולם הסייבר לא מתחילה ונגמרת בהגדרות ובדיקות חוזרות ונשנות. אחד העקרונות המרכזיים ב-ML הוא אכן "לראות" דפוסים של התנהגויות זדוניות, אבל יש צורך גם לצפות פעולות מתקנות. עניין ה"למידה" מגיע ממקום של דפוסים בעייתיים ופתרונם האוטומטי, או לפחות הנפקת רשימת משימות לאדם אשר בעצמו יבצע את סדרת הפעולות הנדרשת. למידת מכונה מתייחסת למחקר, תכנון ופיתוח של אלגוריתמים המעניקים למחשב יכולת ללמוד, וזאת מבלי שהמחשב תוכנת מראש, טכנולוגיה זו תאפשר למחשב לבצע משימות אינטליגנטיות בדומה לאדם, כדוגמת חיזוי, זיהוי, סיווג והכרה.

אפשרויות היישום של ML בעולם הסייבר, תלויות, בראש ובראשונה, בהתקדמות הטכנולוגית שנעשתה בנושא בשנים האחרונות, ובמידת האפקטיביות, או ההתאמה לעולם הסייבר, שהתקדמות זו מביאה עמה. ML בהחלט עשויה להיות אחת הדרכים בה ניתן להגביר את מאמצי האבטחה שלנו.

## להבטיח פריצות דרך משמעותיות

על-פי סקר של Cybersecurity Workforce בשנת 2018, המחסור בכוח אדם מקצועי בתחום הסייבר הגיע לכמעט שלושה מיליון משרות ברחבי העולם. המשיבים לסקר, אשר כולם עוסקים בתחום, ציינו כי יעדיפו להשקיע פחות זמן במשימות אדמיניסטרטיביות ויותר בפעולות הגנת מידע דה-פקטו, אשר מביאות עימן ערך מוסף לעסק, לרבות ניתוח מודיעין, זיהוי איומים, בדיקות חדירה וכדומה.

דוח SBIC מציין, כי זה רק עניין של זמן עד שיצאו לשוק מוצרים מבוססי ML, אשר יהיו זמינים לכל חברה, בכל גודל, בשאיפה להגביר את מאמציהן בתחום הגנת המידע והסייבר. אולם, אחד החסרונות המרכזיים בפתרונות מסחריים, הוא עצם האפשרות, גם של "החבר'ה הרעים", להשיג אותם. עם מספיק נכונות, זמן וכסף, פושעי הסייבר יכולים לבחון היטב את הפתרונות בשוק, "להנדס" אותם ולהפיק תוצאות כזב אשר יעזרו להם לפרוץ למערכות, או לפחות להקשות על תפיסתם. הדרך הטובה ביותר כיום להישאר צעד אחד קדימה, היא לאמץ את גישת הטכנולוגיות המתפתחות ולהטמיע מוצרי AI, ובראשם פתרונות ML, כמוצרים הכרחיים בארסנל הסייבר שלכם.

דבר נוסף שיש לשים לב אליו, הוא מה קורה אחרי הטמעת הטכנולוגיה. ברגע שהוטמעו מודלים של ML, הם הופכים להיות דאטה בפני עצמם, לכן גם עליהם יש להגן כמו על כל שאר הדאטה. מודלים אלה עלולים להוות מטרה ראשונה לתוקפים, ולכן חשוב לתכנן אבטחה לכל שלב בתהליך, לבדוק אותה ולהטמיע אותה בכל התהליכים והכלים התומכים.

האתגר הבולט בתחום הזה הוא הזנה בנתונים "נכונים". במרחב הסייבר יש רגישות נוספת - ייצור נתונים "כוזבים" אשר בסופו של יום ישפיעו על התוצאה. אתגר נוסף הוא יכולת עקיבה, מאחר ואלגוריתמי ML אינם מייצרים לוג שבו ניתן להבין את לוגיקת "ההחלטה" ולקבל רמת דיוק מוגברת.

תפקידה של הבינה המלאכותית ובתוך כך במיוחד תפקידה של ה-ML, הוא להבטיח פריצות דרך משמעותיות בהגנת המידע העסקי. למידת מכונה יכולה להתמקם באחת מנקודות המפתח בעולם אבטחת הנתונים והסייבר - שילוב של כמויות מידע, ניתוחי מידע מתוחכמים, חיזוי ועלייה ניכרת בכוחות המחשוב והענן. כל אלה בעצם מכינים את הקרקע עבור טכנולוגית ה-AI בדרך להיות הלב והמוח של עולם הסייבר, על מלחמותיו.

## לזהות איומים חדשים

ישנו צד תוקף וצד מגן וגם כאן שני הצדדים יעשו שימוש בהתפתחויות שמגיעות מכיוון הבינה המלאכותית. במקום שבו האדם יפסיד, המכונה תנצח. בעוד שמכונות עדיין לא חכמות מספיק בכדי להחליף את הגורם האנושי, הרי שיש להן יתרון משמעותי עלינו. באמצעות שילוב כמות מאסיבית של מידע גלוי עם יכולות הניתוח והמחקר של ML, תוקפים יוכלו לעשות שימוש חכם ביכולות אלה כדי לנתח מידע ולהשתמש בו לצורכי הנדסה חברתית, דבר שיחדד את וקטור התקיפה האנושי ויסייע לתוקפים במאמצי הנדסה חברתית. גם שילוב של כלים מעולמות למידת המכונה העמוקה (DML) מספקים מודיעין נוסף, כיוון שהם יודעים לזהות איומים חדשים על בסיס איתור התנהגות חריגה של משתמשים ברשת ולבצע חיזוי אפשרי למתקפה.

למרות שלמידת המכונה עודנה בשלביה הראשונים בכל הקשור להטמעה עסקית, הפוטנציאל שלה מרגש והיישום שלה בלתי נמנע. הידע שעסקים יכולים להרוויח והפעולות שהם יכולים לנקוט, ידחפו את הארגון קדימה בעולם הסייבר, ויאפשרו לו לצבור יתרונות יחסיים על המתחרים בצורה יעילה ומהירה.

---

הכותבת היא ה-CTO בחברת הסייבר White Hat