Microsoft Security

# מדד אבטחת נתונים

מגמות, תובנות ואסטרטגיות לשמירה על אבטחת הנתונים ולניווט בבינה מלאכותית גנרטיבית

הדוח לשנת 2024

# הקדמה

עם תחילת שנת המחקר השנייה שלנו בנוף אבטחת המידע המתפתח, האתגרים וההזדמנויות העומדים בפנינו מעולם לא היו משמעותיים יותר. בשנה האחרונה חלה עלייה בחומרה של אירועי אבטחת המידע. בעידן זה הממוקד נתונים, האסטרטגיות והכלים המשמשים לשמירה על הנתונים מוגנים מתפתחים בקצב מהיר.

השנה נחקור חזית חדשה: התפקיד וההשפעה של בינה מלאכותית (AI) גנרטיבית על אסטרטגיות אבטחת נתונים.

בינה מלאכותית מכה גלים ברחבי העולם עם יכולות חסרות תקדים שיאפשרו יותר חדשנות ויעילות. בד בבד עם הפוטנציאל העצום הזה, ארגונים חוששים גם לגבי סיכוני אבטחת נתונים והאופן שבו הם עשויים לעצב את תחומי האחריות של צוותי אבטחת מידע. אנו רואים בבינה מלאכותית גורם מאיץ שיאלץ ארגונים לחזק את נוהלי אבטחת הנתונים הבסיסיים שלהם, כך שיוכלו להתכונן למזער את ההשפעה של שיתוף יתר של נתונים ודליפות נתונים, וליצור תהליכים לאימוץ מאובטח של בינה מלאכותית. מצד שני, בינה מלאכותית יכולה גם לעזור לארגונים לשפר את נוהלי אבטחת הנתונים שלהם על-ידי זיהוי סיכונים נסתרים ופערי הגנה, המלצה על מדיניות הגנה, וכן סיוע במחקר ובתיקון מהירים יותר של אירועי אבטחה.

מטרת המחקר שלנו היא לספק למובילי אבטחת נתונים תובנות והנחיות מעשיות שיעזרו לצוותים שלהם להתאים בביטחון את אסטרטגיית אבטחת הנתונים שלהם כדי להגן ביעילות על השימוש בבינה מלאכותית, כמו גם לשלב בינה מלאכותית באסטרטגיות אבטחת הנתונים שלהם. למרות שהיא יוצאת דופן בתפוצה ובפוטנציאל שלה, בינה מלאכותית היא רק גל השינוי האחרון ששוטף ארגונים, כמו עבודה היברידית, ענן וניידות, שבשנים האחרונות הדגיש את הצורך העל-זמני בניראות בשימוש בהם כדי להפחית סיכונים ולמקסם את ההשפעה. בהתבסס על למידה זו, אבטחה נכונה של נתונים המשמשים בבינה מלאכותית, כמו גם שימוש בבינה מלאכותית לשיפור אמצעי אבטחת הנתונים, יאפשרו פרודוקטיביות, עמידות וזריזות רבות יותר כאשר צוותים ינווטו באתגרים עתידיים.

אנו מזמינים אתכם לחקור את הממצאים האחרונים ומקווים כי התובנות יסייעו לכם לחזק את מערך אבטחת המידע שלכם, ובנוסף יעוררו בכם השראה לאמץ בינה מלאכותית ולבנות אסטרטגיית אבטחת נתונים מקיפה, תוך השגת חדשנות רבה יותר והבטחת עתיד בטוח יותר לכולנו.

**Rudra Mitra**
סמנכ"ל החברה
אבטחה ותאימות של Microsoft Data

# מבוא

כאשר ארגונים חווים בממוצע 156 תקריות אבטחת מידע מדי שנה, ההשפעה של תקריות אלה נותרה דאגה מתמדת עבור מקבלי החלטות בתחום אבטחת המידע. יש סיבה טובה לכך: תקרית יחידה עלולה לגרום לנזק כספי ונזק למוניטין עצומים, במיוחד בנוף איומים המתפתח ללא הרף, שבו התוקפים מנצלים את כל נקודות התורפה האפשריות. זה רק הולך וגדל כתוצאה מהאימוץ המהיר של בינה מלאכותית, כאשר ללא הגנות נאותות ואמצעי אבטחה, משתמשים יכולים בטעות או בזדון להציב נתונים קריטיים עסקיים רגישים (כולל מידע על עובדים ולקוחות, קניין רוחני, תחזיות פיננסיות ונתונים תפעוליים), בסיכון. בעוד ארגונים מחפשים דרכים חדשות להגן על מגוון רחב זה של נתונים רגישים, מקבלי החלטות רבים הפנו את תשומת לבם לעלייה הדרמטית של בינה מלאכותית.

אתגר הבינה המלאכותית הוא כפול. בהתחשב בכך ששני שלישים מהארגונים מודים שהעובדים שלהם משתמשים בכלי בינה מלאכותית לא מורשים, זה קריטי שהם יוודאו שהעובדים משתמשים בכלי בינה מלאכותית בצורה מאובטחת. במקביל, יש הזדמנות להשתמש בבינה מלאכותית ככלי יעיל באסטרטגיית אבטחת מידע מתוחכמת.

פתרונות אבטחת נתונים מבוססי בינה מלאכותית כבר ממלאים תפקיד קריטי בזיהוי איומים ובתגובה להם בזמן אמת, משפרים את המהירות והדיוק הכוללים של תוכניות אבטחת נתונים ומספקים תובנות שעוזרות למנוע תקריות אבטחת נתונים לפני שהן מתרחשות. ארגונים מוכרחים לנהל את הסיכונים שהבינה המלאכותית מציגה, בנוסף לרתימת עוצמתה כדי לזהות דפוסים שיכולים להיות מאתגרים עבור בני אדם לעבד ולנתח במהירות מכונה, ובסופו של דבר להילחם במתקפות סייבר מתוחכמות יותר ויותר.

בשנת 2023, Microsoft הזמינה סוכנות מחקר עצמאית, Hypothesis, לערוך סקר רב-לאומי בקרב יותר מ- 800 מומחי אבטחת נתונים ולצאת ביוזמת 'מדד אבטחת נתונים' כדי לשרת טוב יותר את השותפים והלקוחות שלנו ולעזור למנהיגים עסקיים לפתח אסטרטגיות אבטחת נתונים משלהם.

בשנת 2024, דוח זה מתבסס על המחקר הקודם עם תובנות חדשות במסגרת סקר רב-לאומי מורחב של למעלה מ- 1,300 אנשי מקצוע בתחום אבטחת המידע. בעוד הנתונים חושפים תובנות ומגמות עקביות בשווקים שסקרנו, אנו חושפים מידע חדש הקשור לשיטות ומגמות אבטחת הנתונים והבינה המלאכותית העדכניות ביותר ברחבי העולם.

# ממצאים מרכזיים

1

**נוף אבטחת הנתונים נותר מקוטע, מה שמגדיל את הצורך באסטרטגיות אבטחת נתונים מגובשות על פני סיכונים מסורתיים וחדשים הקשורים לשימוש בבינה מלאכותית**

ארגונים מדווחים על רמות גבוהות של שביעות רצון וביטחון באמצעי אבטחת המידע שלהם. עם זאת, חומרת תקריות אבטחת המידע ממשיכה לעלות, בפרט עקב פערים שארגונים מוצאים בין מדיניות אבטחת המידע הנוכחית שלהם לבין השימוש הגובר / ההצגה של אפליקציות בינה מלאכותית. כשהארגונים ניצבים מול סיכונים ועקרונות אלה, רבים מהם עדיין מסתמכים על כלי אבטחת נתונים מרובים שיכולים להגדיל את הפגיעות והסיכון הכוללים שלהם.

2

**ככל שמשתמשי קצה מגבירים את האימוץ של אפליקציות בינה מלאכותית, שלמות הנתונים הרגישים ביותר של ארגונים נמצאת בסיכון גבוה יותר, ודורשת ניראות רבה יותר ובקרות הגנה חדשות**

ככל שכלי בינה מלאכותית הופכים חיוניים לעבודה היומיומית, כך ארגונים מודאגים מסיכוני אבטחת מידע. הם מכירים בצורך לחזק את ההגנות שלהם ומחויבים למנוע אירועי אבטחת מידע הנגרמים על-ידי בינה מלאכותית - אך השימוש הבלתי מורשה בכלים אלה מדגיש את הצורך בניראות חזקה יותר.

3

**מקבלי ההחלטות אופטימיים לגבי הפוטנציאל של בינה מלאכותית להגביר את מאמצי אבטחת המידע שלהם**

ארגונים משקיעים באופן פעיל בכלי אבטחת מידע המשלבים בינה מלאכותית לשיפור יכולות הזיהוי והתגובה. בינה מלאכותית יכולה לעזור לזהות נתונים לא מוגנים, להמליץ על מדיניות הגנה ולעזור לחקור ולתקן אירועי אבטחת נתונים מהר יותר, ובסופו של דבר לאפשר לצוותי אבטחת נתונים למקד יותר זמן ותשומת לב בעבודה אסטרטגית. השימוש בבינה מלאכותית גם מגביר את הביטחון ושביעות הרצון באסטרטגיית אבטחת המידע הכוללת של ארגונים - במיוחד ביכולתם להגיב לאירועים במהירות ובדיוק.

# 1

# נוף אבטחת הנתונים נותר מקוטע, מה שמגדיל את הצורך באסטרטגיות אבטחת נתונים מגובשות על פני סיכונים מסורתיים וחדשים הקשורים לשימוש בבינה מלאכותית

# קיים נתק בין האמון של מקבלי ההחלטות בנוהלי אבטחת המידע שלהם לבין רמת ההגנה האמיתית על הנתונים שלהם

כפי שדווח בשנת 2023, הרוב המכריע של מקבלי ההחלטות בטוחים באסטרטגיות אבטחת המידע שלהם, כאשר 74% דיווחו על שביעות רצון מהפתרונות הנוכחיים שלהם בשנת 2024. הם מרגישים בטוחים ביכולתם לעקוב אחר נתונים רגישים ולנהל אותם: 88% סבורים שהם יודעים היכן נמצא רוב המידע הקריטי שלהם, ו- 85% אומרים שהנתונים שלהם מסווגים ומתויגים כראוי. רובם גם סומכים על בקרות ההגנה שלהם, כאשר 79% בטוחים שהם יכולים למנוע חילוץ נתונים, ו- 76% מתארים את הגישה שלהם כפרואקטיבית ולא תגובתית.

עם זאת, הביטחון שלהם עומד למבחן ככל שחומרת התקרית ממשיכה לגדול. **המספר הממוצע של תקריות אבטחת מידע שנתיות נותר גבוה מ- 166 בשנת 2023 ו- 156 בשנת 2024, וחומרת אירועים אלה עלתה מ- 20% תקריות חמורות ל- 27% בשנת 2024.**

**156**

**תקריות אבטחת נתונים**

**27%**

**מהתקריות נחשבות חמורות**
(עלייה מ- 20% בשנת 2023)

**63%**

**מההתראות נסקרות מדי יום**

"המיקום שבו הוקמה פלטפורמת תוכנה, היכן מאוחסנים הנתונים שלה ומי ייגש לנתונים האלה סיבך את אבטחת המידע והניהול של כלי הבינה המלאכותית והספקים שלנו. יש לנו נתונים השווים ליותר מ- 100 שנה שעלינו להגן עליהם ולפקח עליהם בהתאם לדרישות החוק בכל תחום שיפוט שבו אנו פועלים", אומר מנהל בכיר לפיקוח על מידע ביצרנית ציוד כבד.

העלייה בחומרת אירועי אבטחת המידע הביאה כתוצאה מכך לעלייה בהיקף ההתראות. **ארגונים מתמודדים עם ממוצע של 66 התראות ביום, לעומת 52 בשנת 2023.** מספר זה משתנה באופן משמעותי לפי גודל הארגון, כאשר ארגונים בינוניים (500-999 עובדים) וארגונים גדולים (1,000-4,999 עובדים) מקבלים בממוצע 56 התראות וארגונים גדולים במיוחד (יותר מ- 5,000 עובדים) מקבלים 80 התראות ביום בממוצע.

בהתחשב בכמות העצומה של התראות אבטחת מידע, אין זה מפתיע שרוב הארגונים פשוט לא יכולים לעמוד בקצב. בממוצע, צוותי אבטחת מידע בודקים 63% מההתראות היומיות שלהם. 35% מההתראות הללו מתבררות כחיוביות שגויות. חוסר התאמה זה בין תפיסת השליטה לבין המציאות התפעולית מותיר את צוותי אבטחת המידע המומים – מנסים להעריך אם יש להם את ההגנות הנכונות או כיצד לכוונן אותן, כל זאת תוך חשש שתקריות חמורות עלולות לחמוק בין הכיסאות.

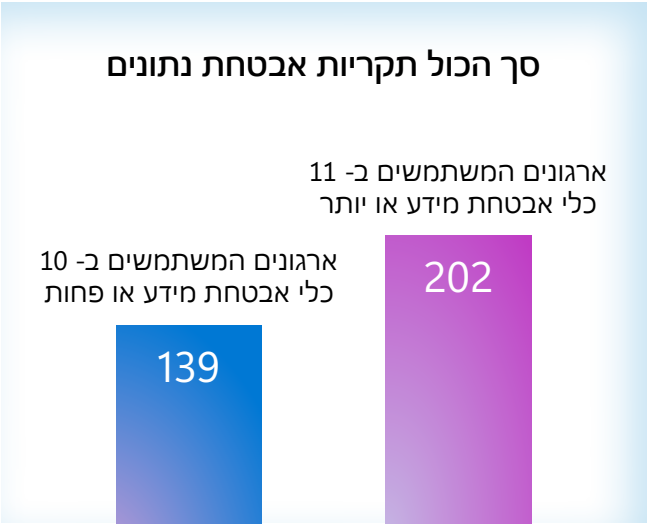
## כדי להילחם בסיכוני נתונים מסורתיים וחדשים הקשורים לשימוש בכלי בינה מלאכותית, יש צורך הולך וגדל באסטרטגיות אבטחת נתונים חזקות ומגובשות יותר

למרות מספרם ההולך וגדל של הכלים העומדים לרשותם, מקבלי החלטות רבים ממשיכים להכיר בכך שיותר אינו תמיד טוב יותר. למעשה, 21% מציינים את ההיעדר של ניראות מגובשת ומקיפה (והבנה משותפת של סיכונים) הנגרם על-ידי כלים שונים כאתגר/סיכון הגדול ביותר שלהם.[1]

רוב מקבלי ההחלטות (82%) מסכימים כי פלטפורמה מקיפה ומשולבת עדיפה על ניהול כלים מבודדים מרובים. **בממוצע, הם מלהטטים בין 12 פתרונות אבטחת נתונים שונים, ויוצרים מורכבות שמגדילה את הפגיעות שלהם.** זה נכון במיוחד בהקשר של הארגונים הגדולים: בממוצע, ארגונים בינוניים משתמשים ב- 9 כלים, ארגונים גדולים משתמשים ב- 11, וארגונים גדולים במיוחד משתמשים ב- 14.

הנתונים מראים מתאם חזק בין מספר כלי אבטחת המידע בהם נעשה שימוש לבין תדירות אירועי אבטחת המידע. ארגונים בינוניים וגדולים מדווחים בממוצע על 89 תקריות בשנה, בעוד ארגונים גדולים במיוחד מתמודדים עם 248 תקריות בשנה. הבדל בולט זה מדגיש את הסיכון הגבוה העומד בפני ארגונים גדולים, גם כאשר הם מביעים אמון רב באמצעי אבטחת המידע שלהם.

בשנת 2024, ארגונים שהשתמשו ביותר כלי אבטחת מידע (11 ומעלה) חוו בממוצע 202 תקריות אבטחת מידע, לעומת 139 תקריות בקרב אלו עם 10 כלים או פחות.




פתרונות מקוטעים מקשים על הבנת מערך אבטחת הנתונים מכיוון שהנתונים מבודדים וזרימות עבודה נפרדות עלולות להגביל ניראות מקיפה של סיכונים פוטנציאליים. כאשר הכלים אינם משתלבים, צוותי אבטחת מידע צריכים לבנות תהליכים כדי לתאם בין נתונים וליצור תצוגה מגובשת של סיכונים, מה שעלול להוביל לשטחים מתים ולהקשות על איתור והפחתת סיכונים ביעילות.

**נושא שמעורר חשש הולך וגדל הוא העלייה בתקריות אבטחת מידע כתוצאה משימוש באפליקציות בינה מלאכותית, שכמעט הוכפלו מ- 27% ב- 2023 ל- 40% ב- 2024.** עלייה זו בתקריות מונעת על-ידי זינוק במתקפות תוכנות זדוניות ותוכנות כופר, עד 59% מ- 50% בשנת 2023. מתקפות כתוצאה משימוש באפליקציות בינה מלאכותית לא רק חושפות נתונים רגישים, אלא גם פוגעות בפונקציונליות של מערכות הבינה המלאכותית עצמן, ומסבכות עוד יותר את נוף אבטחת המידע המקוטע ממילא. בקיצור, יש צורך דחוף יותר ויותר באסטרטגיות אבטחת נתונים חזקות ומגובשות יותר שיכולות להתמודד עם סיכונים מסורתיים ומתפתחים הקשורים לשימוש בכלי בינה מלאכותית.

1. סקר ספטמבר 2024 בקרב מקבלי החלטות בתחום אבטחת מידע, פיקוח, תאימות ופרטיות שהוזמן על-ידי Microsoft מסוכנות MDC Research

## המסלול לקראת העתיד

העלייה בחומרת אירועי אבטחת המידע מצביעה על הזדמנות של בינה מלאכותית לעזור. ארגונים שנמצאים בחוד החנית מיישמים אבטחת נתונים המבוססת על בינה מלאכותית כדי לסייע בתעדוף תקריות, להפוך את סיווג הנתונים לאוטומטי ולזהות דרכים לכוונון עדין של מדיניות ההגנה הנוכחית. בינה מלאכותית יכולה לתרגם באופן אוטומטי את החומרה הפוטנציאלית של התראות על אירועים, ולספק לצוותי אבטחת נתונים תובנות מעשיות לתגובה מהירה כדי להפחית את הזמן המושקע בהתראות שווא. הדבר מייעל את זרימות העבודה ומאפשר לצוותי אבטחת נתונים להתמקד בשיפורים אסטרטגיים יותר באבטחת נתונים ובאמצעים פרואקטיביים.

# 2

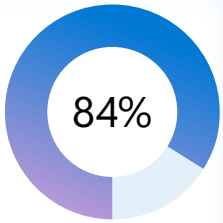
# ככל שמשתמשי קצה מגבירים את האימוץ של אפליקציות בינה מלאכותית, שלמות הנתונים הרגישים ביותר של ארגונים נמצאת בסיכון גבוה יותר, ודורשת ניראות רבה יותר ובקרות הגנה חדשות

# בינה מלאכותית הופכת במהירות לחיונית לעבודה היומיומית - וארגונים חייבים לאמץ ולהסתגל באופן פעיל למציאות חדשה זו

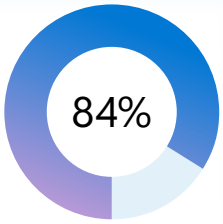
האימוץ המהיר של כלי בינה מלאכותית על-ידי העובדים הביא לשינויים משמעותיים בגישה של ארגונים לאבטחת מידע. בעוד שבינה מלאכותית משנה את הפרודוקטיביות ואת זרימות העבודה, כמו כל טכנולוגיה מתפתחת היא יכולה גם להגביר סיכונים קיימים או להציג סיכונים חדשים הדורשים גישה שונה להגנה על מידע רגיש. כתוצאה מכך, חברות עדיין מוצאות את דריסת הרגל שלהן בנוף המשתנה במהירות. מנהל הנדסה וניתוח בתחום התחבורה טוען: "אנחנו מנטרים נתונים בזהירות רבה יותר בצד הבינה המלאכותית. היה מתח בין פרודוקטיביות לאבטחה, דיוק ופרטיות".

האמון באבטחת השימוש של העובדים בבינה מלאכותית נותר מעורב. הרוב (84%) היו רוצים להרגיש בטוחים יותר לגבי ניהול וגילוי קלט נתונים. בעוד ש- 22% מהארגונים מרגישים בטוחים במיוחד ביכולתם לשמור על אבטחת הנתונים, רובם (59%) הם רק "בטוחים מאוד", מה שמצביע על כך שיש מקום לשיפור. רוב החברות (86%) מודות שהן היו רוצות להרגיש משוכנעות יותר לגבי ניהול וגילוי נתונים שנוצרו על-ידי כלי בינה מלאכותית.

ככל שבינה מלאכותית הופכת חיונית יותר לפרודוקטיביות יומיומית, השימוש באפליקציות בינה מלאכותית הגביר גם את החששות סביב תקריות אבטחת נתונים. **כמעט שליש (31%) מהארגונים צופים עלייה בתקריות אבטחת מידע עקב שימוש העובדים בבינה מלאכותית, ו- 84% מודים שהם צריכים לעשות יותר כדי להתגונן מפני סיכונים אלה.** חששות כאלה גבוהים במיוחד בקרב הארגונים הגדולים: בעוד ש- 26% מהארגונים הבינוניים מצפים לראות עלייה בתקריות אבטחת מידע הקשורות לבינה מלאכותית ו- 29% מהארגונים הגדולים צופים עלייה, קבוצה גבוהה משמעותית המייצגת 36% מהארגונים הגדולים במיוחד צופה עלייה.




**רוצים להרגיש בטוחים יותר לגבי ניהול וגילוי קלט נתונים באפליקציות ובכלים של בינה מלאכותית**




**מסכימים שהם צריכים לעשות יותר כדי להגן מפני שימוש מסוכן של עובדים באפליקציות ובכלים של בינה מלאכותית**

# שימוש לא מורשה בבינה מלאכותית הוא נפוץ

**40% מדווחים שאפליקציות הבינה המלאכותית שלהם כבר נפרצו או נחשפו לסיכון בתקרית אבטחת מידע.** ושוב, נתון זה גבוה יותר בקרב ארגונים גדולים יותר: ארגונים בינוניים מדווחים על שיעור של 36% מהתקריות, ארגונים גדולים מדווחים על 38%, וארגונים גדולים במיוחד ראו את רוב ההתרחשויות, עם 44%.

שימוש לא מורשה בבינה מלאכותית מתרחש לעתים קרובות כאשר עובדים מתחברים באמצעות אישורים אישיים או משתמשים במכשירים אישיים עבור משימות הקשורות לעבודה. **בממוצע, 65% מהארגונים מודים כי עובדיהם משתמשים בכלי בינה מלאכותית לא מורשים.** הדרכים שבהן עובדים משתמשים בכלי בינה מלאכותית לא מורשים כוללות:

- 53% שמתחברים עם אישורים אישיים למטרות עבודה
- 48% המשתמשים במכשיר האישי שלהם בעת שימוש בבינה מלאכותית לעבודה
- 47% המשתמשים באישורי העבודה שלהם כדי להשתמש בבינה מלאכותית למטרות אישיות

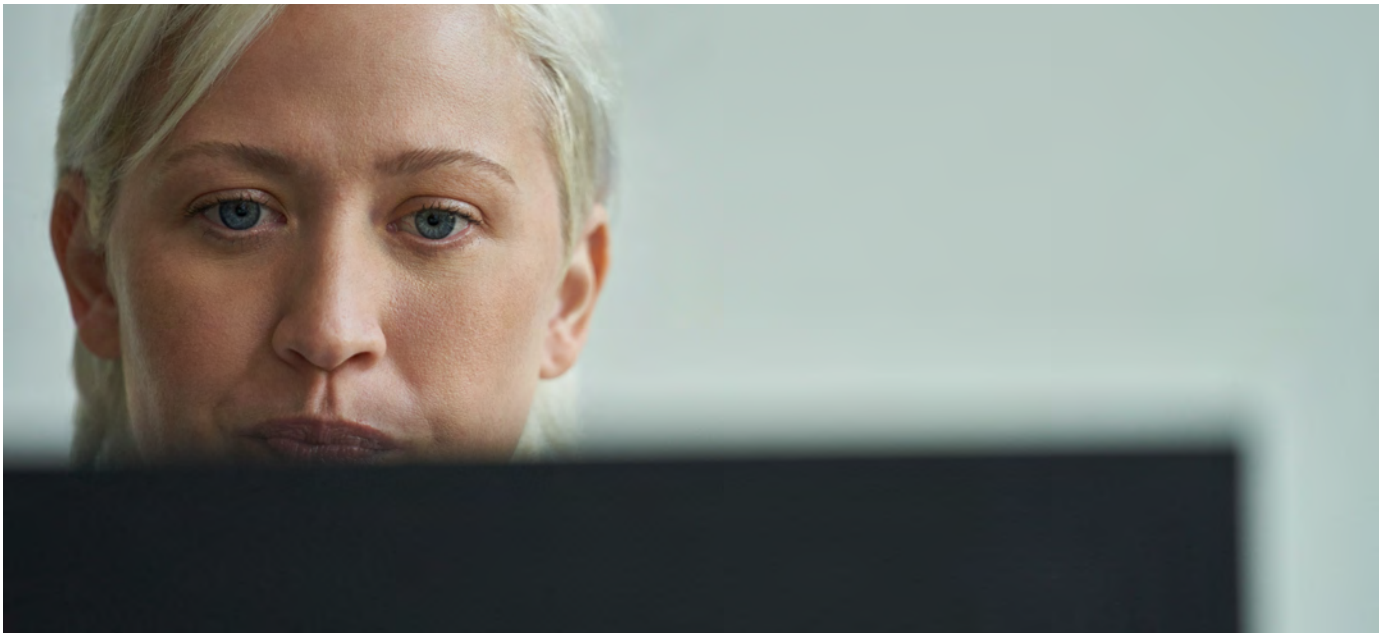
**מחצית מכלל הארגונים אומרים שהם מודאגים מהיעדר בקרות לזיהוי והפחתת סיכונים כאשר עובדים משתמשים באפליקציות בינה מלאכותית בדרכים לא בטוחות.** נתון זה משתנה בהתאם לגודל החברה, כאשר 43% מהארגונים הבינוניים, 50% מהארגונים הגדולים ו- 54% מהארגונים הגדולים במיוחד הביעו חשש לגבי יכולתם לנהל סיכונים אלה.

## בהתחשב בשימוש המוגבר בבינה מלאכותית, יש צורך בבקרות אבטחת נתונים נוספות

ככל שהבינה המלאכותית מוטמעת יותר בפעילות היומיומית, ארגונים מכירים בצורך בהגנה חזקה יותר. **בעוד ש- 96% מהחברות מודאגות לגבי השימוש של העובדים בכלים אלה, מספר כמעט זהה של חברות מוכנות להשקיע בפתרונות כדי להתגבר על החששות שלהן.**

"ההתמקדות הגדולה תהיה באופן שבו מקדימים את הבינה המלאכותית. ההתמקדות של האבטחה היא בהקטנת גודל הנתונים, תוך ניטור נתונים בזהירות רבה יותר. בצד הבינה המלאכותית, כדי להפוך את המודלים שלכם למייצגים יותר לזיהוי הטיה, יש צורך בכמות נתונים גדולה יותר. אז איך מיישבים את זה?", אומר מנהל הנדסה, אדריכלות וניתוח בתחום התחבורה. הרוב המכריע של מקבלי ההחלטות (87%) מוכנים להשקיע זמן וכסף בהדרכת עובדים בשיטות עבודה מאובטחות לשימוש בכלי בינה מלאכותית. **הסיבה לכך היא ש- 85% אומרים שזה קריטי עבור העובדים להשתמש בכלים אלה כדי להישאר תחרותיים.**

כמעט כל הארגונים (93%) נמצאים בשלב כלשהו של פיתוח או יישום בקרות לגבי השימוש בבינה מלאכותית, אך רבים מהם עדיין נמצאים בשלבים המוקדמים. רק 39% יישמו באופן מלא בקרות אבטחת מידע עבור בינה מלאכותית, בעוד ש- 24% פיתחו מדיניות אך עדיין לא יישמו אותה. סמנכ"ל אבטחת מידע בתחום האירוח טוען, "אנחנו מוכרחים ליישר קו עם בקרות לבינה מלאכותית, אבל בינתיים מאמצים את השימוש בבינה מלאכותית. זה אכן משפר את החיים ועוזר לנו להיות יעילים יותר".



בעוד ארגונים נוקטים צעדים כדי להגן על נתונים רגישים מפני שימוש לרעה באפליקציות בינה מלאכותית, יש צורך ברור בבקרות מקיפות יותר. נכון לעכשיו, 43% מהחברות מתמקדות במניעת העלאת נתונים רגישים לאפליקציות בינה מלאכותית, בעוד 42% נוספות מתעדות את כל הפעילויות והתכנים באפליקציות אלה לצורך חקירות פוטנציאליות או תגובה לתקריות. באופן דומה, 42% חוסמות את גישת המשתמשים לכלים לא מורשים, ואחוז זהה משקיע בהדרכת עובדים לשימוש מאובטח בבינה מלאכותית.

לחברות עם עובדים העוסקים בשימוש בלתי מורשה בבינה מלאכותית יש צורך מוגבר בסוגים מסוימים של בקרות. **בקרב אלה עם שימוש בלתי מורשה בבינה מלאכותית, 42% זקוקות לבקרות כדי לזהות משתמשים מסוכנים בהתבסס על שאילתות בינה מלאכותית, לעומת 30% עבור אלה ללא שימוש לא מורשה. יתר על כן, 40% מהארגונים העוסקים בשימוש בלתי מורשה בבינה מלאכותית זקוקים לבקרות לניהול מחזור החיים של נתונים (כגון פרוטוקולי שמירה ומחיקה), בהשוואה ל- 27% מהחברות ללא בעיה זו.**

### 5 בקרות אבטחת המידע המובילות הדרושות

| | |
|---|---|
| מניעת העלאה של נתונים רגישים לבינה מלאכותית | 43% |
| רישום כל הפעילויות והתוכן בכלי בינה מלאכותית לצורך חקירות פוטנציאליות או תגובה לאירועים | 42% |
| חסימת גישת משתמשים לכלי בינה מלאכותית לא מורשים | 42% |
| הדרכת עובדים על שימוש מאובטח בכלי בינה מלאכותית | 42% |
| זיהוי משתמשים מסוכנים בהתבסס על שאילתות לגבי בינה מלאכותית | 41% |

## המסלול לקראת העתיד

כדי לשמור על מערך אבטחת נתונים חזק, צוותים זקוקים לערכה מלאה של בקרות כדי לגלות, להגן ולפקח על הנתונים שלהם באפליקציות הבינה המלאכותית. להלן שלוש אסטרטגיות עיקריות שבהן צוותים יכולים להשתמש:

**שיפור הניראות של השימוש באפליקציית בינה מלאכותית והנתונים הזורמים דרך האפליקציה:** השתמשו בכלי אבטחת נתונים שיכולים לזהות אפליקציות בינה מלאכותית ולהשתמש בהן. כלים אלה מספקים תובנות לגבי רשימה מקיפה של אפליקציות בינה מלאכותית הנמצאות בשימוש יחד עם פרופילי הסיכון שלהן, כולל פרטים כגון בקרות אבטחת נתונים נתמכות ותאימות לתקנות. השתמשו בכלים שיכולים לספק סיווג עקבי עבור נתונים רגישים באינטראקציות בינה מלאכותית, והציגו מגמות לגבי האופן שבו נתונים זורמים דרך אפליקציות בינה מלאכותית.

**פיתוח ואכיפה של מדיניות:** צרו מדיניות המבוססת על התובנות שהושגו מהניתוח. פריטי מדיניות אלה יכולים לכלול הנחיות לאפליקציות בינה מלאכותית מאושרות ונהלים לחסימה או הגבלה של השימוש של עובדים באפליקציות שלא הוטלו עליהן סנקציות. אפילו באפליקציות בינה מלאכותית שהוטלו עליהן סנקציות, ניתן ליצור מדיניות פרטנית שתאפשר לנתונים לא רגישים לזרום דרכן תוך הגבלת השימוש בנתונים רגישים וקריטיים לעסקים. זה יכול לכלול חסימת פעולות מסוימות, כגון הדבקת נתונים רגישים בכלי בינה מלאכותית מבוססי דפדפן כדי להבטיח את אבטחת הנתונים.

**הערכה קבועה של סיכונים וחידוד מדיניות:** צרו באופן קבוע דוחות המציגים את רמות הסיכון של אפליקציות בינה מלאכותית הנמצאות בשימוש, מגמות לגבי האופן שבו נתונים רגישים זורמים דרך אפליקציות אלה, וכן פעילות משתמשים סביב אפליקציות אלה. הדבר מסייע בהערכת נוף הסיכונים הכולל ובקבלת החלטות מושכלות לגבי מדיניות אבטחת המידע הרלוונטית ביותר.

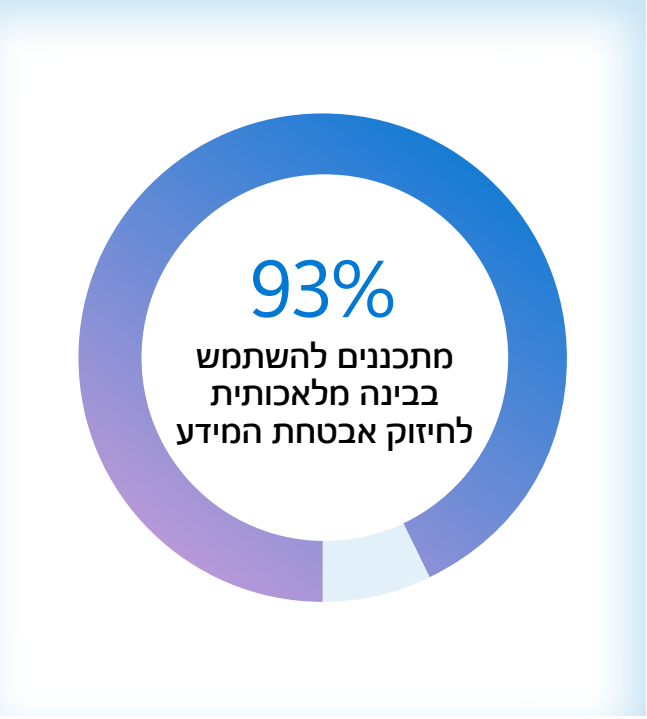
# 3

# מקבלי ההחלטות אופטימיים לגבי הפוטנציאל של בינה מלאכותית להגביר את מאמצי אבטחת המידע שלהם

# חקירות אבטחת מידע מסתמכות במידה רבה על בינה מלאכותית

הרוב המכריע (88%) של הארגונים כבר משקיעים בבינה מלאכותית כדי לשפר את מאמצי האיתור והתגובה שלהם - גילוי נתונים רגישים, זיהוי פעילות חריגה והגנה אוטומטית על נתונים בסיכון. **77% מהארגונים מאמינים כי בינה מלאכותית תאיץ תהליכים אלה, ו- 76% חושבים שזה ישפר את הדיוק של אסטרטגיות הזיהוי והתגובה שלהם.**

**בעוד ש- 73% ממקבלי ההחלטות מביעים חשש משימוש בבינה מלאכותית לחיזוק אבטחת המידע, 50% אומרים שהיא לא עיכבה את השימוש שלהם בבינה מלאכותית לחיזוק אבטחת המידע ורק 23% אומרים שהיא עיכבה אותם. בסך הכל, 93% לפחות מתכננים להשתמש בבינה מלאכותית כדי לחזק את אבטחת המידע למרות החששות.**

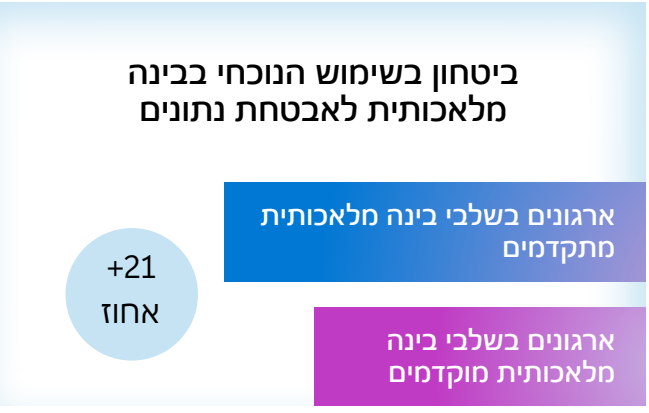



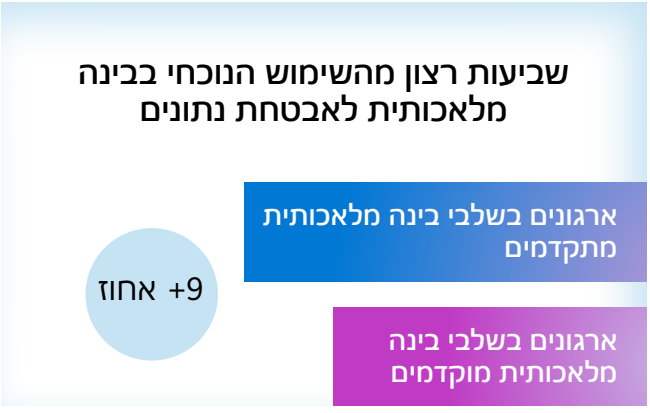
## שימוש בבינה מלאכותית לחיזוק אבטחת הנתונים מגביר את הניראות, הביטחון ושביעות הרצון

אחד היתרונות המרכזיים של שימוש בבינה מלאכותית לחיזוק אבטחת המידע הוא יכולתה להגביר את הניראות בין מערכות, ובכך להפחית חשש בולט שיש למקבלי החלטות לגבי ידיעת מקום האחסון של הנתונים ואופן הסיווג שלהם (20%).[1] 88% ממקבלי ההחלטות בתחום אבטחת המידע מאמינים ששילוב בינה מלאכותית בפתרונות אבטחת מידע יאפשר לצוותים ניראות רבה יותר, שתאפשר לארגונים לעבד ולנתח כמות נתונים גדולה יותר מכפי שהיה אפשרי אחרת. ארגונים בינוניים מתמקדים בעיקר בהפחתת סיכונים לטווח קצר, כגון צמצום טעויות אנוש בתהליכי אבטחת המידע שלהם. למעשה, 43% מהארגונים הבינוניים נותנים עדיפות להפחתת סיכונים הנגרמים כתוצאה מטעויות אנוש, לעומת 37% בלבד מהארגונים הגדולים במיוחד.

לעומת זאת, ארגונים גדולים מתקדמים יותר בגישה שלהם, תוך שימת דגש על סיכונים ארוכי טווח ועל הצורך ביכולת הסתגלות. רמת תחכום מוגברת זו מאפשרת לצוותי אבטחת מידע להסתגל טוב יותר לסיכונים מתפתחים - עדיפות עליונה עבור 49% מהארגונים הגדולים במיוחד, בהשוואה ל- 43% מהארגונים הבינוניים.

בסך הכול, ארגונים שנמצאים בשלב מתקדם יותר בשימוש שלהם בבינה מלאכותית כדי לחזק את אבטחת המידע מדווחים על רמות גבוהות הרבה יותר של ביטחון ושביעות רצון מאסטרטגיות אבטחת המידע שלהם. **בקרב אלו הנמצאים בשלבים מתקדמים של יישום בינה מלאכותית, 90% מרגישים בטוחים במיוחד או מאוד בשימוש שלהם בבינה מלאכותית לחיזוק אבטחת המידע, לעומת 69% בשלבים מוקדמים יותר. באופן דומה, 76% מהארגונים עם שימוש מתקדם בבינה מלאכותית מביעים שביעות רצון מפתרונות אבטחת המידע שלהם, בעוד שרק 67% מהארגונים בשלבים מוקדמים יותר מדווחים על כך.**




1. סקר מספטמבר 2024 שנערך בקרב מקבלי החלטות בתחום אבטחת מידע, פיקוח, תאימות ופרטיות שהוזמן על-ידי Microsoft מסוכנות MDC Research

## ארגונים מצמצמים את מספר תקריות אבטחת המידע ומשפרים את ניהול ההתראות באמצעות בינה מלאכותית

ארגונים המשתמשים בבינה מלאכותית כדי לחזק את פעולות אבטחת הנתונים שלהם מדווחים על פחות התראות באופן משמעותי. **בממוצע, מי שהטמיעו כלי אבטחת מידע מבוססי בינה מלאכותית מקבלים 47 התראות ביום, לעומת 79 התראות למי שלא הטמיע אותם. בנוסף, אלה המשתמשים בבינה מלאכותית מסוגלים לסקור 66% מההתראות היומיות שלהם, בעוד שארגונים שאינם משתמשים בבינה מלאכותית מצליחים לסקור רק 60%.**

בנוסף, אלו המשתמשים בבינה מלאכותית לחיזוק אבטחת המידע נוטים יותר להשתמש גם בבינה מלאכותית כדי להפחית סיכונים (56% לעומת 26%). נראה כי לירידה בהיקף ההתראות, יחד עם היכולת המוגברת למתן אותן באמצעות בינה מלאכותית, הייתה השפעה דרמטית על המספר הכולל של תקריות אבטחת מידע. ארגונים שהטמיעו בינה מלאכותית לחיזוק אבטחת המידע רואים ירידה של 65% בתקריות אבטחת מידע בהשוואה לאלה שאינם משתמשים בבינה מלאכותית לחיזוק אבטחת המידע.

## לבינה מלאכותית צפויה להיות ההשפעה הגדולה ביותר על התגובה

מבחינת זיהוי, 33% ממקבלי ההחלטות מצפים שהבינה המלאכותית תסייע בזיהוי פעילות חריגה, בעוד ש- 23% מאמינים שהיא תסייע בחקירת תקריות אבטחת מידע פוטנציאליות. 22% נוספים רואים את הפוטנציאל של בינה מלאכותית לספק המלצות לאבטחה טובה יותר של סביבות הנתונים שלהם.

עם זאת, התגובה היא המקום שבו מקבלי ההחלטות מצפים שהבינה המלאכותית תשפיע בצורה העמוקה ביותר. 34% מאמינים שבינה מלאכותית יכולה לחסום באופן אוטומטי שיתוף לא הולם של נתונים רגישים, ו- 32% אומרים שהיא תגן על נתונים בסיכון. 26% נוספים רואים שבינה מלאכותית עוזרת להפחית סיכוני אבטחת נתונים ולהחיל בקרות מתאימות, בעוד שמספר זהה מצפה שהבינה המלאכותית תסמן באופן אוטומטי התנהגות מסוכנת של משתמשים.

## המסלול לקראת העתיד

שילוב בינה מלאכותית בפתרונות אבטחת נתונים יכול לעזור בכך שהוא מציע לצוותים הדרכה בזמן אמת, יכולות סיכום ותמיכה בשפה טבעית כדי לשפוך אור על אזורים שאחרת אולי היו זוכים להתעלמות. זה יכול גם להאיץ את החקירה ולחזק את המומחיות בקרב צוותי אבטחת נתונים. כך יכולות אלה עשויות להשפיע:

**סיכום התראות:** חקירות יכולות להיות מרתיעות בשל כמות המקורות לניתוח וכללי מדיניות מגוונים. על-ידי הטמעת בינה מלאכותית במניעת אובדן נתונים (DLP) ובניהול סיכונים פנימיים (IRM), צוותים יכולים לקבל במהירות סיכום של התראות, כולל המקור, כללי המדיניות ותובנות לגבי סיכוני משתמשים כדי להבין אילו נתונים רגישים נחשפו לסכנה ואת סיכון המשתמש המשויך.

**תקשורת הקשרית:** ארגונים מוכרחים לעמוד בדרישות רגולטוריות הנוגעות לתקשורת עסקית, אשר לעתים קרובות מחייבות בדיקה מקיפה של הפרות. בינה מלאכותית יכולה לעזור לצוותי אבטחת נתונים להעריך תוכן מול תקנות ומדיניות ארגונית כדי להדגיש תקשורת בסיכון גבוה שעלולה לגרום לתקרית אבטחת נתונים.

**שפה טבעית לשאילתת מילות מפתח:** חיפוש יכול להיות זרימת עבודה מורכבת שגוזלת זמן רב במהלך חקירות, ואשר דורשת בדרך כלל שימוש בשפת שאילתות של מילות מפתח. בינה מלאכותית מאפשרת לצוותי אבטחת מידע להזין הנחיות חיפוש בשפה טבעית כדי לייעל את תחילת החיפוש ולאפשר חקירות מתקדמות יותר.

# המלצות אחרונות

## 1 התגוננות מפני אירועי אבטחת מידע על-ידי אימוץ פלטפורמה משולבת

אימוץ פלטפורמת אבטחת נתונים משולבת במלואה מציע אסטרטגיה בטוחה ויעילה יותר בסביבה המתפתחת יותר ויותר, מפחיתה את המורכבות ומגבירה את הניראות תוך שיפור ההגנה. גישה משולבת יכולה לסייע לארגונים לשפר את ניהול מצב אבטחת הנתונים על-ידי ריכוז בקרות אבטחת נתונים ומתן ניראות מאוחדת בין נתונים, משתמשים ופעילויות, ובכך לחזק ולייעל את הזיהוי וההגנה סביב סיכוני נתונים. כאשר 82% מהארגונים מסכימים כי פלטפורמה משולבת עדיפה, המעבר לאיחוד אינו רק מועיל - הוא חיוני.

## 2 הגדלת הניראות לגבי השימוש הפנימי בבינה מלאכותית כדי להעריך את הבקרות הדרושות לשימוש העובדים בבינה מלאכותית שלא ישפיעו על הפרודוקטיביות

ככל שבינה מלאכותית הופכת לנפוצה יותר במקום העבודה, היא יכולה להגביר סיכונים קיימים ולהציג סיכונים חדשים. ארגונים מודים שהם צריכים לעשות יותר כדי להגן מפני שימוש לא בטוח בבינה מלאכותית. שימוש בבקרות מוכללות וניראות באפליקציות בינה מלאכותית הוא קריטי כדי לשמור על אבטחת הנתונים מבלי להפריע לפרודוקטיביות. הדרכת עובדים לשימוש מאובטח בבינה מלאכותית יכולה לעזור לארגונים למזער התנהגות מסוכנת תוך הבטחה שהצוותים ימשיכו ליהנות מכלים רבי עוצמה אלה.

## 3 שדרוג אסטרטגיית אבטחת הנתונים בעזרת בינה מלאכותית (AI)

בינה מלאכותית מאפשרת לצוותי אבטחת מידע להתמקד ביוזמות אסטרטגיות יותר במקום להגיב לאיומים מתמידים ולכמות גבוהה של התראות. חברות בשלבים מתקדמים של יישום בינה מלאכותית בטוחות יותר ומרוצות יותר מפתרונות אבטחת המידע שלהן מאשר אלה שרק מתחילות. על-ידי פריסת בינה מלאכותית כחלק מאסטרטגיית אבטחת נתונים מקיפה, ארגונים יכולים לשפר את הניראות שלהם, מה שמחזק את יכולתם לזהות סיכונים ולהגיב להם, ובסופו של דבר לחזק את מערך אבטחת הנתונים הכולל שלהם.

## מטרות המחקר

מטרות המחקר כללו:

1. הבנת נוף אבטחת הנתונים, כולל סדרי עדיפויות ודפוסי חשיבה, אתגרים והגורם וההשפעה של תקריות אבטחת נתונים.
2. גילוי העתיד של אבטחת נתונים, כולל אילו אסטרטגיות וחידושים מופיעים וכיצד ארגונים מתכוונים להשקיע בעתיד.
3. חשיפת תפקידה של הבינה המלאכותית בשיפור אבטחת הנתונים והתפקיד שבינה מלאכותית ממלאת בהגנה על נתונים.

## מתודולוגיה

סקר מקוון רב-לאומי בן 20 דקות נערך בתאריכים 5 עד 23 באוגוסט 2024, בקרב 1,376 מקבלי החלטות בתחום אבטחת המידע.

השאלות נסובו סביב נוף אבטחת המידע ותקריות אבטחת המידע בהשוואה לשנת 2023. בנוסף, הסקר השנה כלל שאלות הקשורות לאבטחת השימוש של העובדים בבינה מלאכותית והשימוש בבינה מלאכותית לחיזוק אבטחת המידע.

## גיוס קהלים

כדי לעמוד בקריטריוני המיון, מקבלי ההחלטות בתחום אבטחת הנתונים צריכים להיות:

- סמנכ"לי מערכות מידע ומקבלי החלטות סמוכים (C-2 ואילך) עם אחריות על אבטחת מידע
- לעבוד בארגונים (500 עובדים ויותר; מגוון גדלים)
- שילוב של תעשיות מוסדרות ולא מוסדרות (לא תחומי חינוך, ממשלה, או ארגונים ללא כוונת רווח)

מתוך 1,376 מקבלי ההחלטות בתחום אבטחת המידע שהשתתפו במחקר, ההשלמות לפי מדינות היו:

- ארה"ב: 302
- בריטניה: 305
- הודו: 301
- ברזיל: 158
- צרפת: 156
- אוסטרליה: 154



Microsoft Security hypothesis