לשכת המבקרים הפנימיים IIA ישראל (חל"צ)
IIA Israel - Institute of Internal Auditors

הכנס המקצועי השנתי של הביקורת הפנימית 2026

Internal Audit NextGen2.0

מעילות והונאות בעידן הAI

כנס מבקרים פנימיים 2026

אורית ולדמן, דירקטורית ביקורת פנים ואחראית על חקירות מעילות והונאות

תקציר

1 מעילות והונאות בתוך הארגון (Internal Fraud)

2 מעילות והונאות מחוץ לארגון (External Fraud)

3 מהפכת ה-AI בעולם המעילות וההונאות

4 אתגרי זיהוי והתגוננות

5 המלצות ומבנה חקירה

סוגי מעילות והונאות – לפי מקור האיום

מעילות בתוך הארגון (Internal Fraud)

- **גניבת נכסים (Asset Misappropriation)**: גניבת מזומן/מלאי, הוצאות כוזבות, החזרי הוצאות, שעות עבודה פיקטיביות
- **שחיתות/ניגוד עניינים (Corruption)**: שוחד, Kickbacks, העדפת ספק, מכרזים "תפורים", קשרים סמויים
- **הונאה בדיווח (Financial/Reporting)**: ניפוח/דחיית הכנסות והוצאות, מניפולציות בדוחות, KPI "מייפים", רישומים לא תקינים
- **מעילות טכנולוגיות מבפנים**: שימוש לרעה בהרשאות, עקיפת בקרות (Override), שינוי נתוני ספק/תשלום, גישה לא מורשית למידע

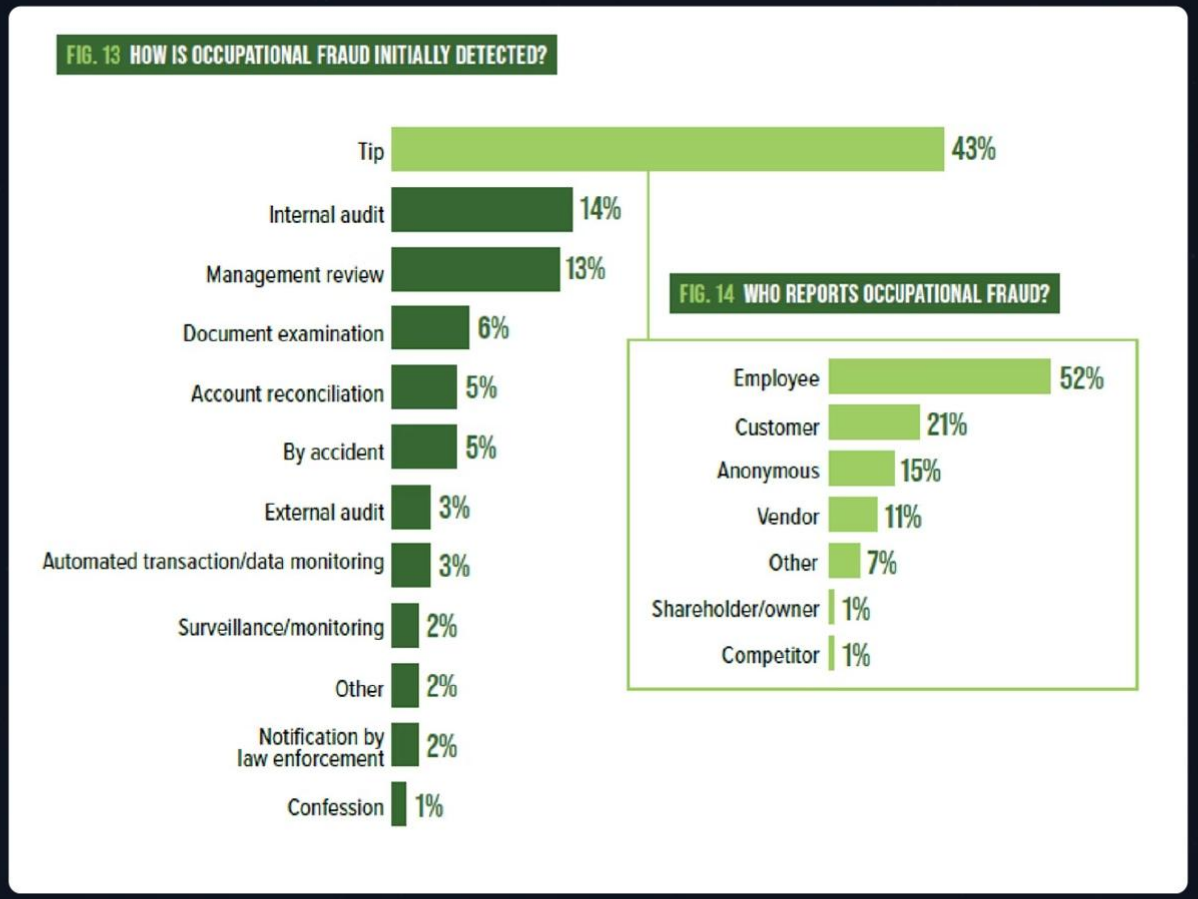
הונאות מחוץ לארגון (External Fraud)

- **התחזות והנדסה חברתית (Impersonation & Social Engineering)**: CEO Fraud/BEC, הונאות תשלום דחופות, זיוף אימייל/טלפון/ווטסאפ
- **סייבר והונאות דיגיטליות (Cyber & Digital Fraud)**: פישינג, Account Takeover, נוזקות, מתקפות על ערוצי תשלום
- **הונאות לקוח/זהות (Customer/Identity Fraud)**: זיוף מסמכים, זהויות סינתטיות, הונאות אשראי/החזרים (Chargeback/Refund)
- **הונאות ספקים חיצוניים (External Vendor Fraud)**: חשבוניות מזויפות, שינוי פרטי בנק, אתרי "ספק דמה"

אזור היברידי – צד ג' (Third Parties / Hybrid)

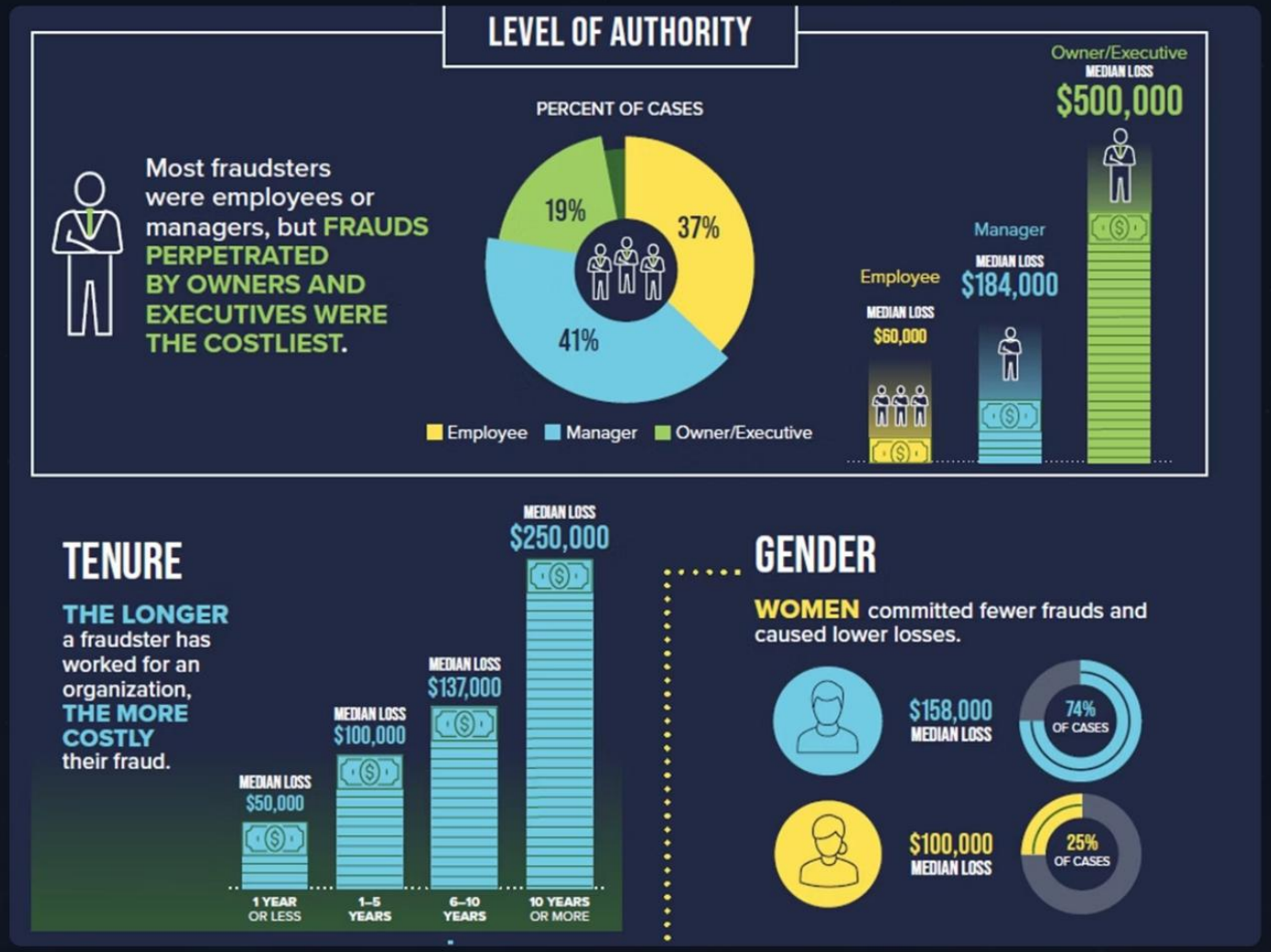
- **גורמים**: ספקים, קבלנים, שותפים, מפיצים — כשיש שילוב של מידע פנימי + גורם חיצוני
- **נקודות תורפה אופייניות**: הקמת ספק, שינוי פרטי בנק, אישור תשלום, קבלת שירות/סחורה

המקור למעילות בתוך הארגון



תוצאות החקירות

פרופיל המועל הממוצע



מבנה חקירת מעילה והונאה

תהליך חקירה מובנה ויסודי חיוני לחשיפת מעילות והונאות, במיוחד בעידן ה-AI המורכב.

קבלת דיווח / ליד

קבלת מידע ראשוני על חשד למעילה ממקורות שונים (עובדים, לקוחות, מערכות ניטור).

הערכה ראשונית ותיעדוף

בדיקה מהירה של המידע, זיהוי אמינותו, והחלטה האם לפתוח בחקירה מלאה בהתאם לסיכון.

איסוף ראיות

איסוף שיטתי של ראיות דיגיטליות (יומנים, תקשורת), מסמכים פיזיים, וגביית עדויות ראשוניות.

ניתוח נתונים וחקירה מעמיקה

בחינה אנליטית של הראיות, שימוש בכלי פורנזיקה דיגיטלית ובינה מלאכותית לזיהוי דפוסים ואנומליות.

ביסוס ואמת הראיות

אימות וחיזוק הראיות שנאספו, בניית תיק חקירה מוצק והכנתו לעימות.

עימות וגביית עדות מהחשוד

הצגת הראיות לחשוד, מתן הזדמנות לתגובה, וגביית עדות רשמית.

סיכום ממצאים והגשת דו"ח

הכנת דו"ח חקירה מפורט הכולל ממצאים, מסקנות והמלצות לפעולה, כולל פנייה לרשויות במידת הצורך.

תפקיד ה-AI בחקירה:

כלי AI יכולים לסייע בכל שלב - מזיהוי אוטומטי של לידים, ניתוח נתונים וזיהוי דפוסים, עד זיהוי דיפ-פייקים וראיות מזויפות. חשוב לשמור על איזון בין אוטומציה של AI לשיקול דעת אנושי.

מהפכת ה-AI בעולם המעילות וההונאות

שינוי חוקי המשחק

בינה מלאכותית משנה באופן דרמטי את עולם ההונאות והמעילות. טכנולוגיות מתקדמות יוצרות אתגרים חדשים שדורשים גישות חדשניות לזיהוי ומניעה.

הונאות מתוחכמות

מועלים משתמשים בכלי AI ואוטומציה שבקנה מידה חסר תקדים המועלים משלבים הנדסה חברתית עם טכנולוגיה מתקדמת.

הצורך בהגנה מתקדמת

מערכי זיהוי ומניעה מתקדמים מבוססי AI הפכו לקריטיים יותר מתמיד. הארגונים שלא יאמצו טכנולוגיות אלה יימצאו חשופים לסיכונים משמעותיים.

מעילות והונאות מחוץ לארגון - External Fraud

סוגים עיקריים של הונאות חיצוניות

פישינג והנדסה חברתית

התקפות ממוקדות להשגת מידע רגיש.

גניבת זהות והשתלטות על חשבונות

גישה לא מורשית לחשבונות משתמשים.

הונאות תשלום וכרטיסי אשראי

שימוש לרעה בפרטי תשלום.

הונאות ספקים

ניפוח חשבוניות או אספקת שירותים פיקטיביים.

מתקפות סייבר ופריצות נתונים

התקפות על מערכות מידע לגניבת נתונים.

הונאות ביטוח

תביעות כוזבות להשגת פיצויים.

הונאות לקוחות

החזרי כספים כוזבים וחיובים חוזרים.

טרנדים מרכזיים במעילות 2024-2025

עלייה של 35% במקרי הונאות AI

קפיצה משמעותית בהונאות המונעות בינה מלאכותית בין 2024 ל-2025, עם מתקפות מתוחכמות יותר המנצלות טכנולוגיות מתקדמות.

שימוש ב-Deepfake

התחזקות שימוש בזיוף וידאו וקול של מנהלים בכירים, יצירת תקשורת מזויפת המאפשרת העברת כספים והונאות מתוחכמות.

זהויות סינתטיות (Synthetic Identity)

גידול בהונאות זהות המורכבות מ-AI, עם יצירת זהויות מלאכותיות מתוחכמות שקשה לזהות ובעלות השפעה ארוכת טווח.

הונאות קריפטו ודיגיטליות

עלייה דרמטית בהפסדים עולמיים המוערכים במיליארדי דולרים, עם ניצול מערכות בלוקצ'יין ומטבעות דיגיטליים.

2025: שנת השיא בהונאות AI

שנת 2025 מסמלת נקודת מפנה קריטית במאבק נגד הונאות בינה מלאכותית, עם התרחבות חסרת תקדים בהיקף, במורכבות ובהשלכות הפיננסיות של האיומים.

היקף פעילות חסר תקדים

עלייה חדה מאוד בהונאות AI וב-Deepfakes אזוריים. התעשייה מאורגנת, משתמשת בכלים זמינים וזולים.

נזק כספי עצום

הונאות AI גורמות לנזקים של מאות מיליונים עד מיליארדי דולרים. מקרים בולטים כוללים תקיפות בתחומי הקריפטו ומקרים רב-לאומיים, עם התרחבות לכל המגזרים.

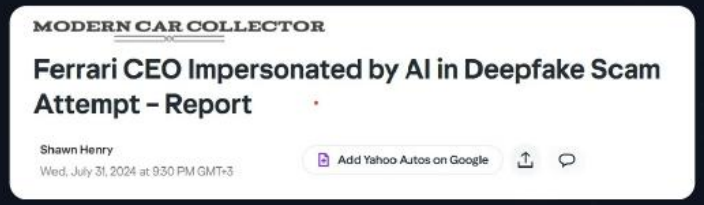
טכנולוגיות AI מתקדמות

שימוש ב-Real-Time Deepfake, זיוף מסמכים אוטומטי, LLM-Scams מתוחכמים ומערכות אוטומציה מלאות מאפשרים הונאות מתוחכמות מאי פעם.

מעגל קורבנות רחב

הקורבנות כוללים את המגזר הפיננסי והממשלתי, עסקים קטנים ובינוניים, תעשיית הקריפטו, סלבריטאים, ואינספור אזרחים פרטיים.

פרסומים מהמדיה על הונאות



הונאת זום בהונג קונג

25 מיליון דולר הועברו לחשבון נוכלים לאחר שעובד פיננסים השתתף בשיחת וידאו עם אווטרים דיגיטליים מזויפים של CFO וחברי הנהלה בכירים.

שנה: 2025

שיטת ההונאה:

- שימוש בטכנולוגיית Deepfake מתקדמת
- יצירת אווטרים דיגיטליים של בכירים בארגון
- ניצול אמון העובד בהנהלה הבכירה
- ביצוע בשיחת וידאו "חיה" שנראתה אמיתית לחלוטין

לקחים:

- אימות זהות רב-שכבתי הכרחי גם בשיחות וידאו
- נהלי אישור מיוחדים להעברות כספיות גדולות
- הכשרת עובדים לזיהוי סימני אזהרה בשיחות וידאו

https://www.youtube.com/watch?v=-kILAg5EBrs

זיוף שידור חי של אילון מאסק

שידור חי מזויף באמצעות דיפ-פייק של אילון מאסק שימש לקידום **הונאת קריפטו** שהונתה אלפי משקיעים ברחבי העולם.

שנה:

2024

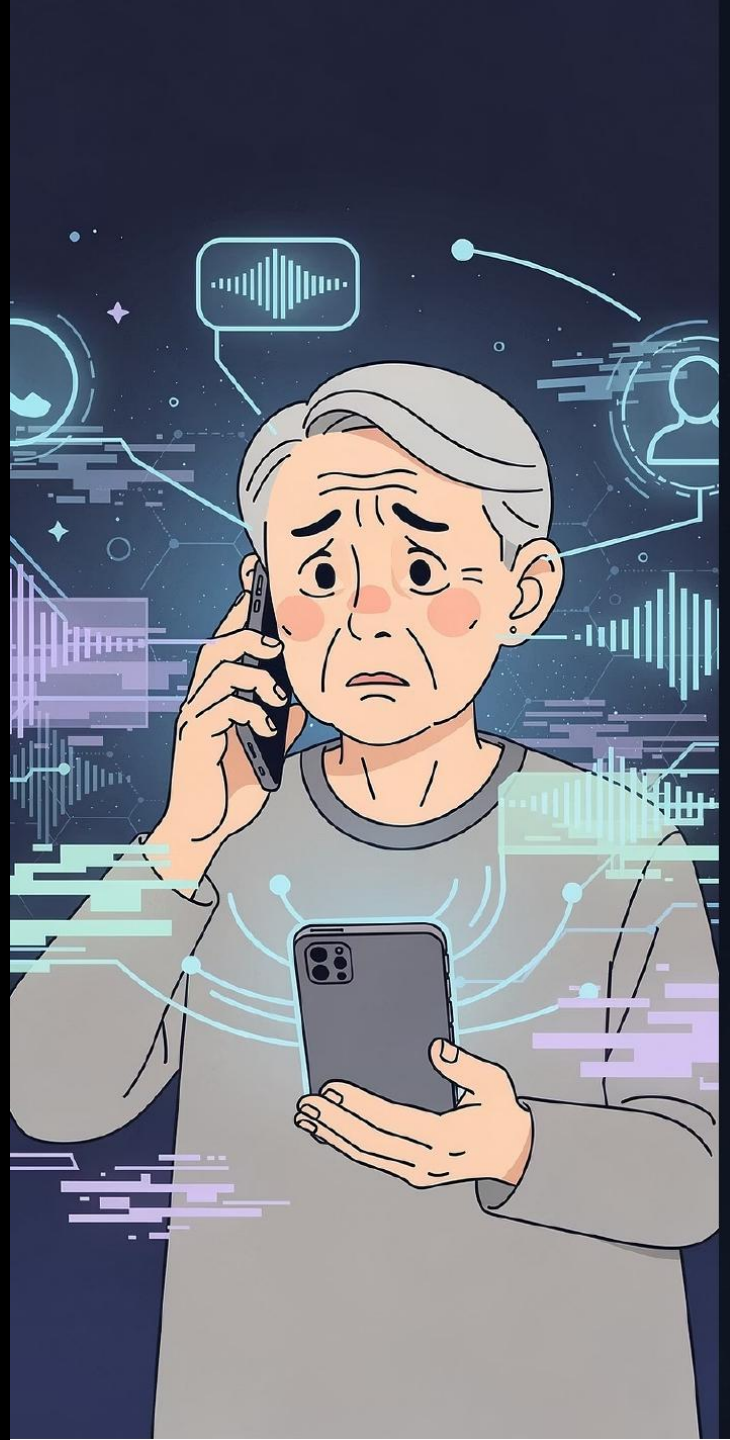
שיטת ההונאה:

- יצירת שידור חי מזויף של אילון מאסק
- קידום הונאת קריפטו תחת מסווה של "השקעה בטוחה"
- ניצול המוניטין והאמינות של דמות ציבורית מוכרת
- הפצה רחבה ברשתות חברתיות ופלטפורמות וידאו

היקף הנזק:

- אלפי קורבנות ברחבי העולם
- הפסדים של מיליארדי דולרים

הונאות קוליות נגד קשישים



זיוף קולי מדויק במיוחד של **בני משפחה במצוקה** לסחיטת כספים מקשישים, תוך ניצול קשרים רגשיים והבטחות לפרטיות.

שנה: 2025

שיטת ההונאה:

- שימוש בטכנולוגיית Voice Cloning מתקדמת
- התחזות לבן/בת משפחה במצוקה
- יצירת תחושת דחיפות ופאניקה
- ניצול הקשר הרגשי והרצון לעזור
- דרישה לסודיות ומהירות בהעברת כספים

אוכלוסיית יעד:

- קשישים - קבוצת סיכון מרכזית
- אנשים עם קשרים משפחתיים חזקים
- אנשים שפחות מכירים טכנולוגיות מתקדמות

אתגרי זיהוי והתגוננות בעידן ה-AI

1

כשל מערכות מסורתיות

מערכות זיהוי הונאות מסורתיות מבוססות כללים סטטיים מתקשות להבחין בין תקשורת אמיתית לזיופים מתוחכמים מבוססי AI, במיוחד כאשר מדובר בדיפ-פייק איכותי.

2

שחיקת האינטואיציה האנושית

אנשים פרטיים מאבדים את "תחושת הבטן" לזיהוי הונאות כאשר הם מתמודדים עם קול מזויף של קרוב משפחה, וידאו משכנע של מנכ"ל, או מסמכים מזויפים בדיוק פוטוריאליסטי.

3

צורך בטכנולוגיות מתקדמות

הצורך הקריטי במערכות זיהוי התנהגותיות בזמן אמת, למידת מכונה מתקדמת, ואלגוריתמי AI שמסוגלים לזהות אנומליות עדינות ודפוסים חריגים.

4

חשיבות ההכשרה והמודעות

הכשרה מתמשכת ומעמיקה של עובדים, מבקרים פנימיים וצוותי אבטחת מידע היא קריטית. מודעות לטכניקות ההונאה העדכניות ביותר יכולה להוות קו הגנה ראשון יעיל.

רגולציה ואכיפה בעידן הונאות AI

התמודדות עם האתגרים המשפטיים והאתיים של הונאות מבוססות בינה מלאכותית מחייבת מסגרת רגולטורית ואכיפתית חזקה ומתפתחת.

תקנות ונהלים לחקירת הונאות AI

פיתוח ויישום נהלים ספציפיים לחקירת מקרי הונאה שבהם מעורבים אלגוריתמים וכלי AI, כולל הנחיות לזיהוי דפוסים חריגים.

דרישות ראייתיות ומשפטיות

הגדרת קריטריונים ברורים לאיסוף, שימור, וניתוח ראיות דיגיטליות ממערכות AI, תוך שמירה על שרשרת אבטחה (Chain of Custody) מחמירה.

סמכויות חוקרים ומבקרים

הרחבת סמכויות מבקרים פנימיים וחוקרי הונאות, והכשרתם בכלים לניתוח נתוני AI וזיהוי מניפולציות אלגוריתמיות.

שיתוף פעולה עם רשויות אכיפה

חיזוק הקשר ושיתוף המידע בין ארגונים פרטיים לרשויות אכיפת החוק, כולל משטרה, בנקים מרכזיים וגופים בינלאומיים.

תיעוד ושמירת ראיות דיגיטליות

חובה על ארגונים לתעד פעילות מערכות AI, לשמור יומני אירועים (Logs) ומטא-דאטה, ולאפשר גישה מבוקרת לראיות במקרה של חקירה.

מערכות זיהוי אנומליות בעידן ה-AI

התאמות נדרשות למערכות מידע קיימות

ניטור AI בזמן אמת

יכולות ניטור משופרות לזיהוי וניתוח תוכן שנוצר או שונה על ידי AI (כולל דיפ-פייק וקול סינתטי), יחד עם מעקב רציף אחר שימושים חריגים ובלתי צפויים במערכות AI.

ניתוח התנהגותי מותאם

ניתוח התנהגותי של משתמשים ומערכות, תוך התחשבות בדפוסי אוטומציה של AI.

אינטגרציה וזיהוי מתקדם

הטמעה של כלים ייעודיים לזיהוי AI (למשל, זיהוי דיפ-פייק ואימות תוכן סינתטי), לצד שילוב והצלבת מידע ממגוון רחב של מקורות נתונים לאימות וגילוי אנומליות.

מאפיינים של מערכות מודרניות לזיהוי הונאות

מודלי למידת מכונה

מודלים מאומנים לזהות דפוסי הונאה מבוססי AI מתפתחים.

אימות ביומטרי והתנהגותי

טכניקות אימות חזקות לאבטחת זהויות ומניעת התחזות.

איתור אנומליות בעסקאות AI

זיהוי חריגות בעסקאות שבוצעו באמצעות מנגנוני AI.

מערכות התראה מתקדמות

התראות מיידיות על שימוש חשוד בכלי AI ופעילות חריגה.

אינטגרציה מלאה

שילוב חלק עם מערכות ERP, CRM ומערכות פיננסיות קיימות.

המלצות

המלצות להתמודדות ומבט לעתיד

הטמעת מערכות AI

זיהוי הונאות בזמן אמת ושיפור תהליכי בקרה באמצעות בינה מלאכותית

חקיקה ורגולציה

איזון בין חדשנות טכנולוגית להגנת צרכנים

הכשרת מבקרים

הכשרה מתמשכת להתמודדות עם אתגרי AI

ארגונים שיאמצו גישה פרואקטיבית, ישקיעו בטכנולוגיות מתקדמות, ויטפחו תרבות ארגונית של ערנות ומודעות - הם אלה שיצליחו להתמודד בהצלחה עם אתגרי העתיד.

העתיד כבר כאן

מהירות חסרת תקדים

ה-AI משנה את פני ההונאות והמעילות במהירות שלא ראינו מעולם. הטכנולוגיה מתפתחת מהר יותר מיכולת הארגונים להגיב.

תפקיד המבקר הפנימי

המבקר הפנימי חייב להיות שותף פעיל במאבק, מצויד בכלים טכנולוגיים מתקדמים וידע עדכני בטכניקות הונאה חדשניות.

הובלת המאבק

מי שיאמץ טכנולוגיות מתקדמות, יגבש אסטרטגיות חדשניות, וישקיע בהכשרה מתמשכת - יוכל להוביל את המאבק בהונאות ולהפוך לדוגמה לחיקוי.

הזדמנות וסיכון

שני צדדים של אותה מטבע דיגיטלית: הטכנולוגיה שמאפשרת הונאות היא גם הטכנולוגיה שתאפשר לנו להדוף אותן.

תודה על ההקשבה

אורית ולדמן 0526458746