מערכת לזיהוי והערכת האימפקט הפיננסי הצפוי מאירועי סייבר

מהות המערכת

המערכת הינה פלטפורמה מבוססת מתודולוגיה מובנית ויכולות בינה מלאכותית המיועדת לזהות ולהעריך את ההשפעה הפיננסית הפוטנציאלית של אירועי סייבר על הכלכלה של ישראל. המערכת סורקת באופן אוטומטי מקורות מידע מגוונים בזמן אמת, מבצעת סינון וקטגוריזציה של האירועים באמצעות מודלי למידת מכונה, ומנתחת את פוטנציאל ההשפעה על פי מערכת כמותית של מדדים משוקללים. מה שמייחד את המערכת הוא יכולתה לשלב מידע חיצוני עם נתונים ממקורות מגוונים ולהפיק התראות ממוקדות לבעלי תפקידים שונים על פי חומרת האימפקט הפיננסי הצפוי והרלוונטיות שלו לכלכלה בישראל. המערכת כוללת ממשק משתמש אינטראקטיבי המאפשר למומחים אנושיים לבחון, לעדכן ולשפר את ההערכות האוטומטיות, ובכך יוצרת לולאת משוב מתמשכת המשפרת את הדיוק והרלוונטיות לאורך זמן.

נחיצות המערכת

המערכת תציף פוטנציאל השפעה על הכלכלה ברמה הלאומית כתוצאה מאירועי סייבר גלובליים על ידי:

- זיהוי אותות אזהרה מוקדמים: לאירועי סייבר יש לעתים קרובות השפעות מצטברות שאינן גלויות באופן מיידי. המערכת מעריכה אירועים אלה באופן שיטתי כדי לזהות איומים פוטנציאליים על היציבות הפיננסית של ישראל לפני שהם מתממשים, או קרוב להתרחשותם.
- טיפול בפגיעויות חוצות-מגזרים: כלכלות מודרניות מקושרות יותר ויותר. למשל, מתקפה על תשתיות אנרגיה בצפון אמריקה או על ספק תוכנה באירופה עלולה להיות בעלת השלכות בלתי צפויות על היציבות הכלכלית של ישראל.
- סטנדרטיזציה של הערכת השפעה :המערכת מספקת גישה עקבית ומתודית להערכת אירועי סייבר מגוונים במגזרים, באזורים גיאוגרפיים וקטורי תקיפה שונים.
- גישור על פערי מידע: המערכת יוצרת צינור מובנה בין מידע על אירועים מסוגים שונים ומאיזורים שונים ומתרגמת אותם להערכת סיכונים פיננסיים, ומבטיחה שמידע טכני מתורגם לתובנות פעילות עבור המנהיגות הפיננסית.

הצעת ערך

המערכת מספקת ערך באמצעות:

- הערכת סיכונים כמותית: על ידי הקצאת ציונים ספציפיים במספר ממדים, היא מתרגמת מידע איכותני על איומי סייבר למדדי סיכון כמותיים ובכך מקבלי החלטות פיננסיות יכולים לפעול על פיהם.
- תעדוף משאבים: רמות הסף המדויקות (קריטי, גבוה, בינוני, נמוך, מינימלי) מסייעות למקבלי ההחלטות להקצות משאבים מוגבלים ביעילות במהלך מספר אירועים בו-זמנית.
- מוכנות משופרת: מוסדות פיננסיים ורגולטורים יכולים להכין תוכניות פעולה על בסיס אזהרות מוקדמות, ובכך למנוע/להכיל נזק כלכלי.
- כיסוי מקיף: המערכת מתייחסת לכל תחום, החל מתחכום ההתקפה ועד להשפעות על השוק הפיננסי.
- חוסן פיננסי לאומי: על ידי מתן אזהרות מוקדמות על איומים פוטנציאליים, המערכת מחזקת את יכולתה של ישראל לשמור על יציבות פיננסית במהלך התרחשות אירועי סייבר גלובליים מהותיים.

סקירה פונקציונאלית של המערכת

פונקציות עיקריות <u>לשלב ראשוני</u> של הקמת והעמדת המערכת:

- איסוף נתונים בזמן אמת -

- איתור מידע רלוונטי ממקורות זמינים בזמן אמת, בשלב ראשוני לפחות ממקורות ציבוריים או כאלו שיש להם API זמין
- יכולת לאסוף מידע לפחות מ 6 שפות: עברית, אנגלית, ערבית, צרפתית, ספרדית, רוסית

- ניתוח מבוסס בינה מלאכותית -
  - יכולת עיבוד וניתוח מבוסס AI של המידע על בסיס מודל הערכת פוטנציאל השפעה על המערכת הפיננסית המוצע, עם יכולת הערכה של 90% ומעלה
  - יישום מדדים לאמוד את הפלט הכוללת הערכת הזיות, רצף לוגי, פרשנות שגויה של קלט / קלט חלקי.
- אינטגרציות לשימוש במקורות מידע פנימיים -
  - יכולת לקבל מידע ממקורות פנימיים בשלב ראשוני (לדוגמה: מידע מהמרכז לסייבר פיננסי)
  - עיבוד מידע סטאטי בשלב ראשוני (מסמכים, טבלאות וכו)
- הפעלת התראות -
  - יצירת התראות, מסוג push, התראת דוא"ל והתראת in-app.
  - תוכן התראה הוא גנרי בשלב ראשון
  - יכולת לשלוח התראה לכל מי שהוגדר על ידי האדמין
- ממשק משתמש -
  - בניית מערכת מבוססת Role Base. בשלב ראשוני בעלי הגישה השונים הם: אדמין, משתמש מסוג Viewer, משתמש מסוג Reviewer
  - דשבורד - בשלב ראשון לאפשר תצוגות בסיסיות מוגדרות מראש (אירועים אחרונים, ניקוד אירוע, פירוט מלא, תובנות בסיסיות).
  - יכולת חיפוש ופילטור- מבוססת פילטור על שדות קבועים
  - יכולת ייצוא דוחות - בשלב ראשוני בסיסית (למשל או לפי אירוע, או לפי רמת סיכון, או לפי זמן, וכו)
  - רספונסיבי וב/מובייל - בסיסי בשלב ראשוני (עבור תצוגות מוגדרות בלבד).
  - יכולת הטמעה / white labeling - הממשק יותאם לאינטגרציית מחלקת פיננסים-סייבר.
  - <u>פעולות על ידי משתמש מסוג Reviewer-</u>
    - הוספה/עריכת מקורות, בשלב ראשוני יכולת הוספה בלבד, דורש אישור אדמין.
    - ייצוא דוחות - בשלב ראשוני ייצוא דוחות בסיסיים מוגדרים מראש.
- ממשק אדמין -
  - יכולת להזמין משתמשים, לקבוע את סוג ההרשאה, בשלב זה רק מיילים מדומיינים מוגדרים מראש. יכולת להסיר משתמשים או לאקטב הזמנה שפגה תקופה
  - תצוגת Insights ואנליטיקות
  - ייצוא דוחות - כמו מהממשק משתמש
  - יכולת לערוך או להוסיף מקורות ידע
- ביצועי **AI** ושיפורים מתמשכים -
  - למידה תקופתית, הלוקחת גם משוב של משתמשים מסוג Reviewer המפדבקים את הערכות המערכת לאירועים, ויישום על מיפוי הניקוד למדדים וקטגוריות.

פירוט פונקציות עיקריות לשלב ראשוני של הקמת והעמדת המערכת:

1. איסוף ידיעות בזמן אמת

איסוף בזמן אמת ממקורות מרובים מאפשר זיהוי של איומי סייבר מתפתחים ואירועים לפני או בזמן קרוב להתרחשותם ועל מידת השפעתם על הכלכלה בישראל, מהלך זה, מספק זמן מקדים קריטי לאמצעי מניעה והבלה. גישת ניטור מקיפה זו קולטת נקודות מבט מגוונות על אירועי סייבר.

סוגי מקורות: תקשורת חדשותית; מקורות ממשלתיים; מקורות ביטחוניים; סוכנויות בינלאומיות; מקורות סייבר; מכוני מחקר; פלטפורמות מודיעין; רשתות חברתיות; דארק וב, וכו',

שיקולים:

- חלק מהמקורות הם ציבוריים, וחלקם מוגבלים בגישה
- חלק מהמקורות ידרשו חשבונות פרימיום

2. ניתוח ראשוני למידע שנסרק

הניתוח הראשוני מסנן תוכן נכנס באמצעות מודל סיווג קל שמזהה אירועי סייבר בביטחון של לפחות 75%, תוך שהוא מבטל כפילויות על בסיס קריטריונים נוקשים של דמיון ומקור. שלב סינון קריטי זה מבטיח שרק אירועי סייבר רלוונטיים, בפועל או פוטנציאליים, ממשיכים להערכה עתירת משאבים, ובכך מפחית באופן משמעותי עלויות עיבוד ומונע עומס התרעות.

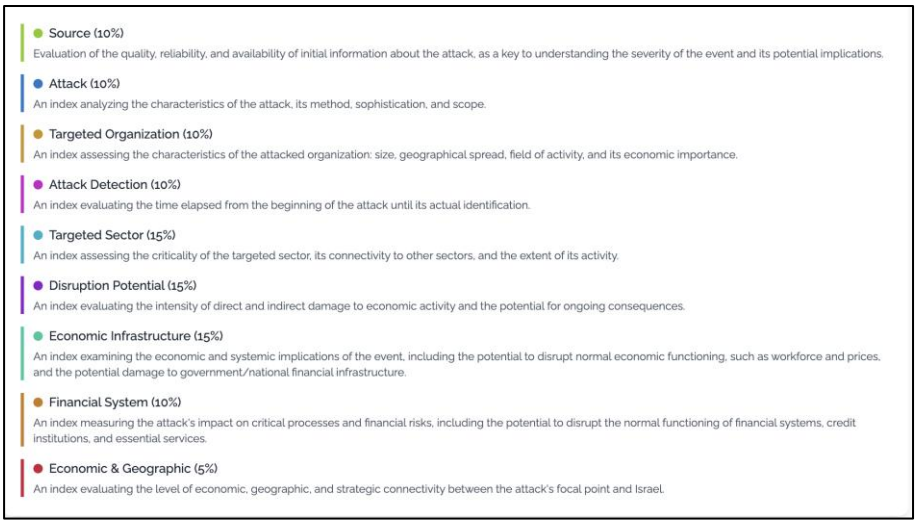
Commented [1]: TBD

3. מידע שנסרק נכנס לתוך מחולל הערכת פוטנציאל ההשפעה על המערכת הפיננסית של ישראל

מערכת הערכת ההשפעה על הכלכלה מייצגת מערכת אנליטית מקיפה המיועדת להעריך ביצד אירועי סייבר המתרחשים עשויים להשפיע על היציבות הפיננסית והתשתית הכלכלית של המדינה.
ליבת המערכת מעסיקה מתודולוגיית ניקוד רב-שכבתית המעריכה תחילה את מאפייני אירוע הסייבר (אמינות המקור, תחכום ההתקפה, פרופיל הארגון הנפגע ולוח הזמנים לגילוי), ולאחר מכן מעריכה את ההשפעה הפוטנציאלית ספציפית על המערכת הפיננסית של ישראל.

המערכת פועלת על ידי קליטת נתונים ממקורות חיצוניים מרובים (במפורט במסמך זה) והצלבת מידע זה עם נתונים פנימיים מגורמים שונים כפי שיוגדרו. הצלבה זו מספקת מודעות הקשרית לחשיפה ופגיעויות ספציפיות על הכלכלה בישראל.
הניתוח של המערכת מופעל על ידי מערכות בינה מלאכותית מתקדמות שמעבדות באופן רציף דוחות נכנסים, מנקדות אוטומטית אירועים לפי מדדי מפתח עם הקטגוריות-המשנה שלהם, ומזהות דפוסים שאנליסטים עלולים להחמיץ. מנוע הבינה המלאכותית מעשיר את ההערכה על ידי למידה מתמשכת ובכך משפר את יכולות החיזוי שלו.

המדדים המשוקללים מבחינים בין מאפייני האירוע (40% מההערכה) להשפעות פוטנציאליות ספציפיות לישראל (60% מההערכה), ומייצרים הערכת סיכון החל מ"מינימלי" ועד "קריטי". גישה זו מאפשרת למקבלי ההחלטות להעריך ולתעדף אילו אירועי סייבר מצדיקים תשומת לב מוגברת, הכנה או אמצעי תגובה בכלי עזר לשכבות ההגנה על היציבות הפיננסית של ישראל.



בעת פיתוח מערכת הערכת ההשפעה הפיננסית של מתקפות סייבר, יהיה צורך להתמודד עם מספר אספקטים הנוגעים לדיוק המערכת:

- דיוק הניקוד: לאמת ולזקק את המשקל היחסי של מדדים וקטגוריות-משנה באמצעות בדיקות רטרוספקטיביות נרחבות מול אירועי סייבר היסטוריים עם השפעות פיננסיות ידועות, להבטיח שהמערכת מייצרת הערכות התואמות לתוצאות בעולם האמיתי.
- טיפול במקרי קצה :
  - יישום פרוטוקול פורמלי לאירועים שאינם מתאימים בצורה ברורה לקטגוריות-משנה קיימות, כולל תהליך טיפול בחריגים סטנדרטי המאפשר לאנליסטים לתעד נימוקים להחלטות ניקוד מותאמות אישית תוך שמירה על עקביות ההערכה.
  - השארת "באפר" לבינה מלאכותית בו, במקרי הצורך, יוצעו או יזוהו קריטריונים חדשים שהמודל לא התייחס אליהם עד כה. במקרים כאלו יבחנו ההצעות על ידי גורם אנושי מוסמך לפני יציאת ההתראה ויאושרו / יוטמעו או יידחו.
- התייחסות לאירועים בהם חלה התפתחות תוך זמן קצר: פיתוח יכולת הערכת סדרות זמן המאפשרת ניקוד מתקדם ככל שאירועים מתפתחים, כולל הערכות בגרסאות שונות, מדדי ביטחון המשקפים שלמות מידע, ומנגנוני הערכה מחדש אוטומטיים כאשר מופיע מידע חדש משמעותי.
- מיפוי תלויות: בניית קשרים מקיפים בין מדדים כדי לקחת בחשבון אפקטים מצטברים, כאשר השפעות בתחום אחד עשויות להגביר או למתן השפעות באחרים.
- הפחתת אזהרות שווא: שילוב מנגנוני אימות להפחתת הסבירות להשפעות מוגזמות, על ידי ביול הערכת אמינות המקור הראשונית מול אישורים עובדתיים עוקבים.
- מערכת התאמה: יצירת מחזור סקירה פורמלי למתודולוגיית הניקוד עצמה, המאפשרת למערכת להתפתח ככל שמופיעים וקטורי תקיפה חדשים ומערכות פיננסיות משתנות.
- יכולת למידה מתמשכת של ה **AI** מתוך אינפוט משתמשים ומקרי בוחן נוספים, ושיפור הדיוק של יכולות המערכת
- איתור הזיות בפלט ה **LLM** טיוב תשובות ומערכת בקרה פנימית על הפלט של הLLM
- מנגנון מעטפת של "הסבר" המציג למשתמשים הסבר על הלוגיקה ושימוש במקורות מידע של ה LLM

כללי שמירה מבוססי ניקוד (הצעה לדיון נוסף) :

Commented [2]: TBD

הניקוד המשוכלל שיינתן מהמודל ימופה לרמות קריטיות שונות, המשקפות את מהירות הדיווח עליהן, בעלי העניין שיקבלו את הדיווח, ופעולות נוספות אשר יתבצעו בהתאם:

- קריטי (85-100): אחסון קבוע עם בדיקות עדכון יומיות
- גבוה (65-84): שמירה של 180 יום עם בדיקות עדכון שבועיות
- בינוני (50-64): שמירה של 90 יום עם בדיקות עדכון דו-שבועיות
- נמוך (35-50): שמירה של 45 יום עם בדיקות עדכון חודשיות
- מינימלי (<35): שמירה של 14 יום ללא בדיקות עדכון

טריגרים נוספים לעדכון בעלי העניין :

Commented [3]: TBD

- יוגדרו תוך כדי הרצת מקרים רבים במערכת לצורכי דיוק המערכת.
- טריגרים לדוגמה שנוכל לשקול: שינוי ציון משמעותי (10± נקודות); התייחסות למידע חדש מאירועים קשורים; הארכה מפורשת על ידי אנליסטים

4. שליחת התראות לבעלי תפקידים שונים -

מטרה: להעביר את המידע הנכון לבעלי העניין הנכונים בזמן הנכון. ספי התראה וערוצי העברה הניתנים להתאמה על בסיס תפקידי בעלי עניין, תחומי אחריות, והעדפות אישיות.

תנאי טריגר: ספי ניקוד (לפי הרמות המפורטות מעלה) וערכי רכיבים ספציפיים
התאמה אישית: ערוצי העברה (פוש נוטיפיקיישן לטלפון, מייל), תדירות (אירועים קריטיים ידווחו מיידית לעומת אירועים עם

פוטנציאל מינימאלי), ורמת פירוט לפי בעל העניין (האם יקבל פירוט מלא על האירוע או דוח סיכום שבועי מתומצת)
תבנית: תבניות מוגדרות מראש עם ויזואליזציה של ניקוד וממצאים עיקריים

הגדרה:

Commented [4]: TBD

- אילו בעלי עניין מקבלים אילו סוגי התראות
- מתי הם מקבלים התראות
- מה תוכן ההתראה
- מהן פעולות המעקב

תהליך לדוגמה -

אירוע סייבר בחברת שינוע סחורות בינלאומית - ניתוח האירוע ומתן ציון - משלוח מייל לכל הגורמי שטח, איסוף פידבקים - ביצוע הע"מ - הפצת תוצרים לרשימת תפוצה - כינוס פורום מתאים לפי רמת חומרה.

לדוגמה:

סוג האירוע	רמת חומרה	מנגנון הפצה	משתתפים לפעולה	משתתפים לידיעה
אירוע סייבר בחברת דלק גדולה בארה"ב	נמוך	מפ"ל/משרד האוצר	מערך סייבר חירום ובטחון באוצר	תת ועדת סייבר בוועדת היציבות
אירוע סייבר בבנק אירופי גדול	בינוני	מפ"ל/מנכ"ל האוצר	ראשי אגפים באוצר, אגף חירום בבנק ישראל	רפרנט חירום באגפי האוצר ובב"י/מזכירות ועדת היציבות
אירוע סייבר בחברת שינוע סחורות ימית גדולה	גבוה	מפ"ל/שר האוצר	שר האוצר/נגיד בנק ישראל	ב"י/רח"ל/מס"ל

כללי - דשבורד משתמש

<u>ממשקים ממוקדי בעלי עניין שונים</u>

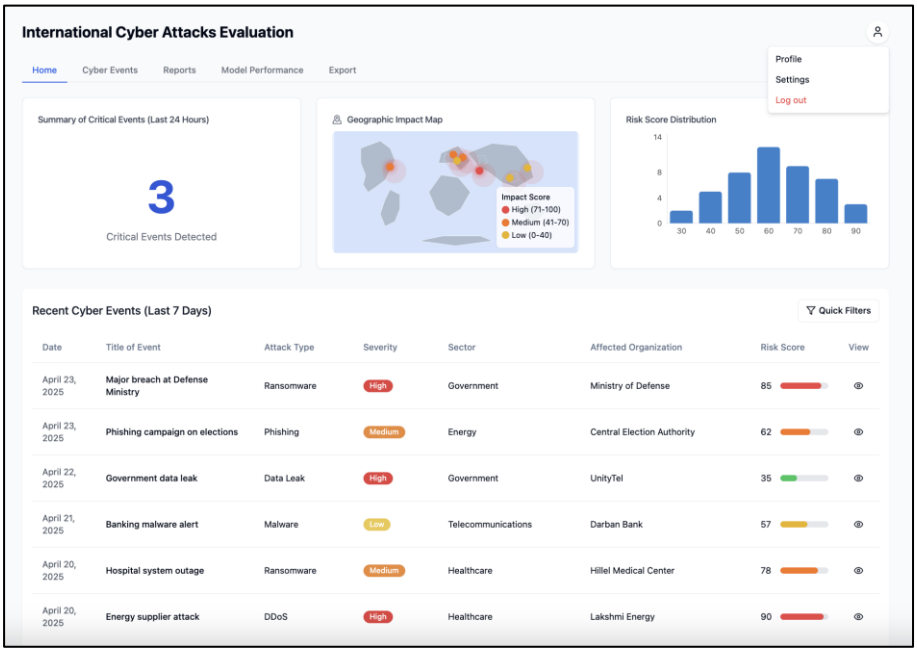
מטרה: להציג מידע בפורמטים המותאמים לצרכי משתמש שונים ורקעים טכניים.

פונקציונליות ליבה:

- מרכז מידע מאוחד: מקנה תצוגה מאוחדת של ארועי הסייבר הרלוונטיים לכלכלה של ישראל. מקור מאוחד לכל אירועי הסייבר עם פוטנציאל השפעה כלכלית/פיננסית, מאחד הערכות ממערכות אוטומטיות ומומחים אנושיים עם הבחנה ברורה בין הערכות מאומתות לראשוניות.
  - יש להגדיר:

Commented [5]: TBD

    - לאילו בעלי עניין יש גישה אליו
    - אילו תצוגות יהיו זמינות ובאיזו רמה
- ממשק סקירת אירועים: תצוגה מפורטת של כל הערכה עם נתוני מקור
- בקרות התאמת ניקוד: כלים אינטראקטיביים לכל מדד מערכת
- תיעוד הנמקה: שדות טקסט למעריכים אנושיים לתיעוד הנמקה
- אימות מקור: קישורים למקורות המקוריים עם הדגשת מידע חיוני
- קישוריות: מחברים לאירועים קשורים וקשרים פוטנציאליים
- המערכת צריכה להיות בעלת יכולת להתממשק בדרך אחת או אחרת למערכת "תמונת מצב כללית"



אבטחה וגישה

מטרה: להבטיח הגנה מערכתית חזקה תוך שמירה על יעילות תפעולית. מיישם אמצעי אבטחה מקיפים להגנה על מידע רגיש, מאזן בקרות גישה קפדניות עם חוויית משתמש. שומר על יומני גישה מפורטים למטרות ציות וביקורת אבטחה.

- יישום **FA2**: נדרש לכל המשתמשים
- ניהול סשן: הגדרת פסק זמן אוטומטי לאחר חוסר פעילות (בהגדרה מראש)
- ניהול רישום התחברות ונסיונות התחברות: כל ניסיונות התחברות ושימוש בכלי הממשק יהיו מתועדים

דף הבית

מטרה: לספק מודעות באמצעות סיכומי אירועים באופן טקסטואלי וויזואלי. לספק תמונת מצב מיידית של מצב האירועים באמצעים ויזואליים המפנים תשומת לב למידע הקריטי.

לדוגמה:

- פאנל תובנות מפתח (לדוגמה, יוגדר בהמשך):
  - סיכום אירועים קריטיים (24 שעות אחרונות)
  - ויזואליזציה של מגמות בסוגי אירועים
  - מפת השפעה גיאוגרפית
  - תרשים התפלגות ציוני סיכון
- טבלת דוחות אחרונים (לדוגמה, יוגדר בהמשך):
  - עמודות הניתנות למיון לפי תאריך, חומרה, קטגוריה, מגזר יעד

- דשבורדים דרגות חומרה ויזואליים
- קישורים לגישה מהירה לדוחות מלאים
- אפשרויות סינון מהיר

לשונית דוחות

- מטרה: לאפשר חקירה מפורטת וניתוח שיתופי של אירועים בודדים. ישלב פונקציונליות חיפוש רחבה, עם פרטי אירועים מקיפים, יאפשר לאנליסטים לבחון איומים ספציפיים. יטפח ידע שיתופי באמצעות מיפוי הקשרים, הוספת הערות וכו'.
- חיפוש וסינון מתקדמים: לאפשר מיקוד של אירועים רלוונטיים בתוך נפחי נתונים גדולים. יאפשר לאנליסטים לאתר במהירות אירועים ספציפיים או דפוסים באמצעות קריטריונים מרובים, עם תכונות התאמה אישית (בגון חיפוש שמור וסינון מבוסס תגיות) לתמיכה בצרכי מיפוי מידע חוזרים.
- תצוגת פרטי דוח: להציג מידע מקיף על האירוע עם הקשר ושקיפות הערכה. יספק ויזיביליות מלאה (בולל לינקים לידיעה המקורית) להערכות אירוע עם מעקב ביקורת של התראות ושינויים, ויאפשר תמיכה בקבלת החלטות מושכלת ואחראית.
- פאנל אירועים קשורים: לזהות דפוסים וקשרים שעשויים להצביע על אירועי סייבר קשורים. נשתמש באנליזה מתקדמת כדי לחשוף קשרים בין אירועים, יסייע לזהות אירועי סייבר מתוחכמים.
- הערות ושיתוף פעולה: לאפשר ניתוח מבוסס צוות ושימור ידע. יוצר סביבה מובנית לאינפוטים מבעלי עניין שונים, ישמר ידע ארגוני ויאפשר תמיכה רציפה בתגובה לאירועים בין צוותים שונים.

Commented [6]: TBD

לשונית ביצועי מודל

מטרה: לספק שקיפות לגבי איכות הערכת בינה מלאכותית ומגמות שיפור. מציע נראות לאמינות המערכת האוטומטית באמצעות מדדי ביצוע, בונה אמון בפלטפורמה ומדגיש תחומים לשיפור.

לדוגמה, יוגדר בהמשך: ציוני ביטחון בחיזוי; שיעורי חיוביים/שליליים שגויים; מגמות שיפור לאורך זמן; מתאם אמינות מקור...

פונקציונליות ייצוא

מטרה: לאפשר אינטגרציה עם מערכות חיצוניות (שליחה בדוא"ל וכו') ודיווח לבעלי עניין. תומך במגוון פורמטים פלט ואפשרויות התאמה אישית כדי לענות על צרכים תפעוליים מגוונים, מאינטגרציות טכניות ועד תדריכים למנהלים, וכן פונקציונליות אוטומציה. המערכת צריכה לאפשר ייצוא בהתאמה לדרישות פנימיות או לאפשר התממשקות עם API.

ממשק אדמין (מנהל המערכת)

ניהול משתמשים ותפקידים

מטרה: לשמור על אבטחה באמצעות בקרת גישה מדויקת ופיקוח מקיף. מספק למנהלים כלים לשליטה בהזמנות משתמשים, להבטחת גישה מתאימה על בסיס תפקידים ארגוניים, ולניטור שימוש במערכת למטרות אבטחה.

דוחות

מטרה: לנטר את בריאות המערכת, ביצועים ודפוסי שימוש. מספק תובנות לביצועים טכניים והתנהגות משתמשים כדי לאפטמל את תצורת המערכת, לזהות צרכי הדרכה, ולהבטיח שהפלטפורמה עומדת בדרישות תפעוליות.

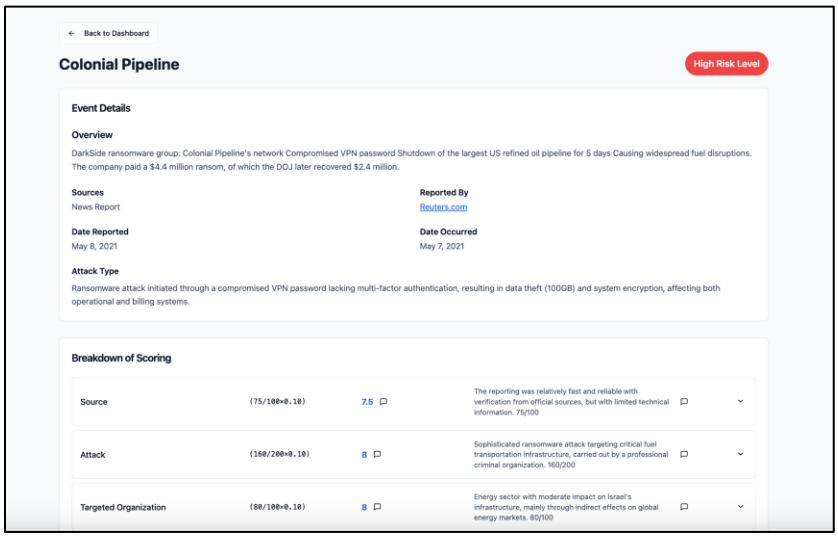
תובנות מערכת

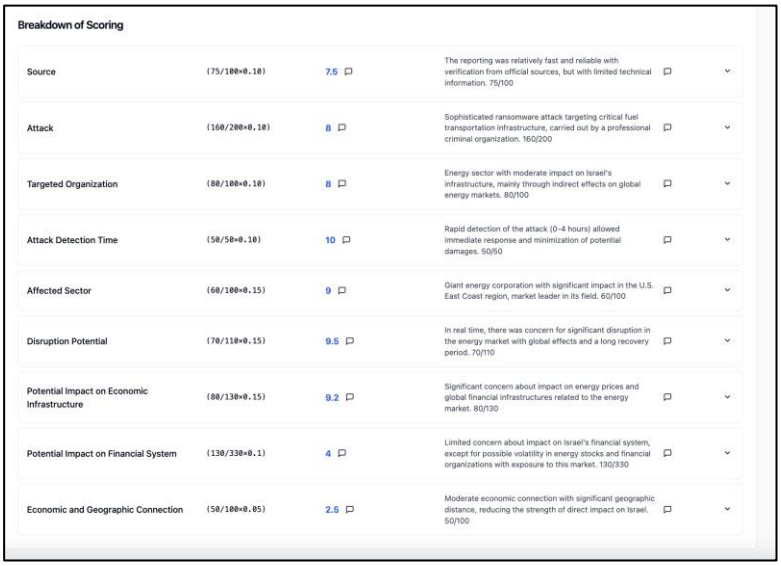
מטרה: לזהות באופן פרואקטיבי ארועי אבטחה במערכת והזדמנויות לאופטימיזציה. משלב ניטור אבטחה (התחברויות שנכשלו, דפוסי גישה חריגים, אנומליות וכו') עם אנליטיקת שימוש (דוחות הנצפים ביותר; דפוסי חיפוש נפוצים; וכו') כדי להגן מפני איומים תוך שיפור מתמשך של הפלטפורמה על בסיס דפוסי שימוש בפועל. בנוסף מבסה יומני שגיאות עיקריים, התראות עדכוני מודל, וכו'.

אינטגרציית מנגנון המאפשר Human-in-the-loop: מערכת אינטראקטיבית בין בעלי התפקידים ל - AI

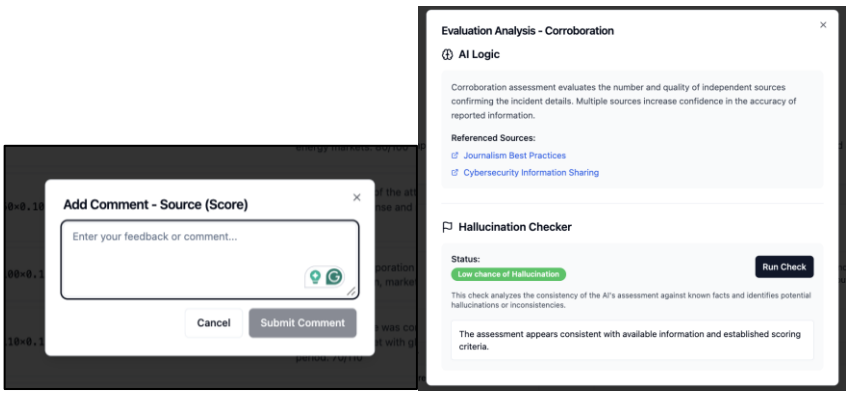
מטרה: למנף את האפקטיביות הטכנולוגית והמומחיות האנושית לצורכי הערכת פוטנציאל נזק אופטימלית.
מנגנוני סקירה אינטואיטיביים מאפשרים למומחים אנושיים לאמת או להתאים הערכות אוטומטיות, ולמקד את תשומת הלב במקומות בהם יוכלו להוסיף ערך, תוך שמירה על כיסוי מקיף באמצעות אוטומציה.

- מערכת ניהול משימות ופרטי מידע - יש לפתח יכולת ניהול משימות ושיתוף פרטי מידע בין משתמשי המערכת בסגנון **Ticket / Monday / Jira** וכו)
- מערכת למידה מתמשכת
  - מטרה: להבטיח שהפלטפורמה מתפתחת ומשתפרת באמצעות שימוש, איסוף משוב מובנה המשפר את דיוק ההערכה לאורך זמן, מסתגל לדפוסי אירועים חדשים ומשפר חיזויי השפעה בהתבסס על תוצאות בפועל של אירועים קודמים.
  - בשלב ראשוני, למשתמשים בעלי הרשאה מסוג reviewer ,תיפתח האפשרות להכניס משוב באיזורים מוגדרים (ניקוד כללי למדד, ניקוד לקטגוריה, משוב להסבר, וכו).
  - המשתמשים יוכלו להריץ בדיקות הזיות, לקבל הסבר לאופן בו בוצע הניתוח וכולה.
  - המערכת תאסוף את המשובים ובאופן תקופתי שיוגדר תשתמש בהם כחלק משיפורים תקופתיים למודל.




Breakdown of Scoring
Source (75/100×0.10) 7.5 The reporting was relatively fast and reliable with verification from official sources, but with limited technical information. 75/100
Attack (160/200×0.10) 8 Sophisticated ransomware attack targeting critical fuel transportation infrastructure, carried out by a professional criminal organization. 160/200
Targeted Organization (80/100×0.10) 8 Energy sector with moderate impact on Israel's infrastructure, mainly through indirect effects on global energy markets. 80/100
Attack Detection Time (50/50×0.10) 10 Rapid detection of the attack (0-4 hours) allowed immediate response and minimization of potential damages. 50/50
Affected Sector (60/100×0.15) 9 Giant energy corporation with significant impact in the U.S. East Coast region, market leader in its field. 60/100
Disruption Potential (70/110×0.15) 9.5 In real time, there was concern for significant disruption in the energy market with global effects and a long recovery period. 70/110
Potential Impact on Economic Infrastructure (80/130×0.15) 9.2 Significant concern about impact on energy prices and global financial infrastructures related to the energy market. 80/130
Potential Impact on Financial System (130/330×0.1) 4 Limited concern about impact on Israel's financial system, except for possible volatility in energy stocks and financial organizations with exposure to this market. 130/330
Economic and Geographic Connection (50/100×0.05) 2.5 Moderate economic connection with significant geographic distance, reducing the strength of direct impact on Israel. 50/100


Breakdown of Scoring
Source (75/100×0.10) 7.5 The reporting was relatively fast and reliable with verification from official sources, but with limited technical information. 75/100
Detailed Breakdown - Source
Metric Category Points Explanation Feedback Evaluation
Speed of Reporting Two-day reporting window 20 reporting with a delay of approximately 2 days
Reliability Case study 25 a credible primary journalistic source
Technical Detail Comprehensive 15 Provides technical details yet not in detail
Corroboration Multiple sources 15 Article cites multiple corroborating sources


Add Comment - Source (Score)
Enter your feedback or comment...
Cancel
Submit Comment
Evaluation Analysis - Corroboration
AI Logic
Corroboration assessment evaluates the number and quality of independent sources confirming the incident details. Multiple sources increase confidence in the accuracy of reported information.
Referenced Sources:
Journalism Best Practices
Cybersecurity Information Sharing
Hallucination Checker
Status:
Low chance of Hallucination
Run Check
This check analyzes the consistency of the AI's assessment against known facts and identifies potential hallucinations or inconsistencies.
The assessment appears consistent with available information and established scoring criteria.

פונקציות נוספות מומלצות כפיתוח המשך

- מנגנון הערכת נזק כספי/תפעולי תכונה זו תספק אומדנים כמותיים של הפסדים פיננסיים פוטנציאליים מאירועי סייבר, ותאפשר תכנון תקציב והקצאת משאבים. היא תשתלב עם מודלים כלכליים ונתוני הפסד היסטוריים כדי ליצור תחזיות השפעה כספית.
- כלי ניתוח תרחישים עתידיים יכולות מידול מתקדמות יפתחו תרחישים שונים של התפתחות התקפות והשפעותיהן המדורגות על המגזר הפיננסי של ישראל. ניתוח חיזויי זה יאפשר תכנון פרואקטיבי על ידי חקירת מצבי "מה אם", ויאפשר למקבלי החלטות להכין תוכניות למספר תוצאות פוטנציאליות. (סימולטור)
- הערכת השפעה מצטברת (אירועים מרובים/בו-זמניים) יכולת זו תנתח את ההשפעות המשולבות של אירועי סייבר בו-זמניים או רצופים, תוך הכרה שהתקפות בעולם האמיתי מתרחשות לעתים קרובות בגלים. המערכת תמדל כיצד מערכות מבוזרות מתקשרות ומחמירות סיכונים, ותספק הערכה קרובה למציאות של פגיעויות מערכתיות בתקופות משבר.
- מערכת התרעה מוקדמת לאיומים מתפתחים אלגוריתמי למידת מכונה יזהו דפוסים וחריגות שקודמים לאירועי סייבר גדולים, ויספקו אזהרה מוקדמת לפני שהאירועים מתממשים. יכולת חיזויית זו תנתח מגמות, מתודולוגיות התקפה ומדדים גיאופוליטיים כדי לחזות סיכונים מתפתחים למגזר הפיננסי של ישראל.
- ניתוח מגמות ודפוסים ארוכי טווח ניתוח נתונים היסטוריים יחשוף נופי איום מתפתחים ומגמות תחכום התקפות על פני תקופות ממושכות. תכונה זו תתמוך בתכנון אסטרטגי על ידי זיהוי דפוסים מחזוריים, וקטורי התקפה מתפתחים ושינויים ביכולות השחקנים בראיה צופה פני עתיד.
- יכולות שיתוף פעולה בין-ארגוניות מנגנוני שיתוף מידע יאפשרו הגנה מתואמת על פני מוסדות מרובים תוך שמירה על דרישות סיווג ופרטיות נתונים. זה ייצור רשת מודיעין שיתופית בין מוסדות פיננסיים, סוכנויות ממשלתיות ושותפים בינלאומיים למודעות מצבית משופרת.
- הרחבת סיכון חוץ פיננסים (סח"פ) המערכת תתרחב מעבר לארועי סייבר כדי לכלול סיכונים נוספים שעלולים להשפיע על יציבות פיננסית, כגון אסונות טבע, מגפות או אירועים גיאופוליטיים. גישת הערכת סיכון מקיפה זו תספק תצוגה מאוחדת של כל האיומים על חוסן המגזר הפיננסי.

מיפוי דרישות טכנולוגי

1. תשתית איסוף נתונים:
   - מערך סוכני בינה מלאכותית אוטונומיים המתוכננים לסריקה יזומה של מקורות מידע מגוונים, כולל יכולת התאמה דינמית למבנה משתנה של אתרים
   - מנגנוני תזמון ותיעדוף חכמים המבוססים על רלוונטיות מקורות
   - יכולות API לגישה למקורות בתשלום
   - מנגנוני הטמעה ייעודיים לדארק וב ורשתות חברתיות
2. מערכת עיבוד וקטורי:
   - תשתית מסדי נתונים וקטוריים לאחסון ואחזור יעילים
   - אלגוריתמים לזיהוי דמיון וקשרים בין אירועים
   - יכולות לאחזור סמנטי ומבוסס הקשר
3. מערכת בינה מלאכותית והערכה:
   - מודלי סיווג לזיהוי אירועי סייבר רלוונטיים המבוססים על סטים מתויגים של אירועי סייבר היסטוריים, עם מנגנון אימון מחדש תקופתי המשלב אירועים חדשים שזוהו ואומתו בידי מומחים
   - מנגנוני הערכת השפעה מבוססי מדדים משוקללים התואמים את מערכת הניקוד שהוגדרה, עם יכולת עדכון משקולות בהתאם למשוב והתפתחות האיומים
   - יכולות NLP מתקדמות לניתוח טקסט לא מובנה, כולל זיהוי ישויות, ניתוח סנטימנט, זיהוי יחסים סמנטיים, והבנת הקשר בין אירועים, תוך התמודדות עם שפות מרובות ותחום ידע ספציפי לסייבר
   - מנגנוני זיהוי הזיות וטיוב תוצאות המשלבים אימות צולב ממקורות מרובים, איתור סתירות וחוסר עקביות בתוצאות, וכלים סטטיסטיים לזיהוי תשובות בהסתברות נמוכה או בעלות מורכבות חריגה
   - מערכת הסבר לוגי (Explainable AI) המספקת שקיפות להחלטות המודל, תוך פירוט המקורות, המשקולות והחישובים שהובילו לניקוד הסופי, באופן המאפשר למשתמשים להבין את הרציונל מאחורי כל הערכה
   - מערכת מעקב וניטור מתמשכת אחר ביצועי מודלי ה-LLM, כולל זיהוי חריגות, מדידת רמות דיוק ומהימנות, וניתוח האינטראקציות עם משתמשים לזיהוי נקודות שיפור ובעיות פוטנציאליות
4. ממשקי אינטגרציה:
   - חיבורים מאובטחים למקורות מידע פנימיים
   - ממשקים לשליחת התראות במגוון פלטפורמות (דוא"ל, SMS, אפליקציות מובייל)
5. תשתית אבטחת מידע:
   - מערכת אימות דו-שלבית (FA2) עם אפשרויות מרובות (SMS, אפליקציה, מפתח פיזי)
   - הצפנת נתונים בתנועה ובמנוחה עם מפתחות ייעודיים לכל סוגי המידע
   - ניהול הרשאות מבוסס תפקידים עם גרנולריות גבוהה
   - מנגנוני ניטור ורישום פעילות מקיפים כולל ניתוח אנומליות בזמן אמת
   - עמידה בתקני אבטחת מידע והגנת פרטיות הנדרשים בישראל (רמו"ט/PMEO), האיחוד האירופי (GDPR) וארה"ב (כגון NIST, CCPA), תוך התמקדות בהגנה על מידע רגיש וזכויות הפרט
6. תשתית למידה מתמשכת:
   - מנגנון לאיסוף משוב ממשתמשים
   - יכולות עדכון מודלים ושיפור ביצועים אוטומטיים
   - מערכת תיעוד וקטלוג של הערכות היסטוריות
7. ארכיטקטורת ממשק משתמש:
   - ממשקים מותאמים אישית לסוגי משתמשים שונים על בסיס תפקיד והרשאות
   - יכולות ויזואליזציה מתקדמות המציגות תמונת מצב בזמן אמת ומגמות היסטוריות
   - כלים אינטראקטיביים להתאמת ועדכון הערכות כולל אפשרויות משוב מיידי
   - מערכת דוחות מתקדמת עם יכולות יצירת דוחות מותאמים אישית, תצוגה מקדימה ושמירת תבניות
   - מנגנוני ייצוא במגוון פורמטים (PDF, Excel, CSV, JSON) עם אפשרויות התאמה אישית לשדות ולתקופות
   - ממשקי אינטגרציה (API) לחיבור למערכות חיצוניות כגון מערכות SIEM, פלטפורמות BI, ומערכות ניהול אירועים ארגוניות

ארועי סייבר עם השפעות כלכליות חוצות גבולות

ארועי סייבר לדוגמה:

SolarWinds - 2020

- מקור: בעיקר יעדים בארה"ב
- השפעה חוצת גבולות: מתקפת שרשרת האספקה השפיעה על ארגונים ברחבי העולם
- השפעה כלכלית מחוץ למקור:
  - בלגיה: מוסדות האיחוד האירופי שהשתמשו ב-SolarWinds נתקלו בחששות אבטחה ועלויות תיקון
  - בריטניה: סוכנויות ממשלתיות ועסקים הוציאו מיליונים על תגובה לאירוע
  - קנדה, מקסיקו, ספרד, ישראל, איחוד האמירויות: מוסדות פיננסיים רבים ספגו עלויות משמעותיות לחקירה ותיקון
- דווח על ידי Politico
-

מדד	חישוב	הסבר ניקוד משוקלל
מקור (10%)	8	מקור (8.0): אמינות גבוהה של המידע מחברות סייבר מובילות וגופי ממשל אמריקאיים.
התקפה (10%)	8.25	התקפה (10.0): מתקפת סייבר מדינתית מתוחכמת שהצליחה לחדור דרך עדכוני תוכנה לגיטימיים.
ארגון נתקף (10%)	9.5	ארגון נתקף (9.5): פגיעה בחברת תוכנה גלובלית עם לקוחות בכל העולם, כולל גופים פיננסיים.
משך גילוי התקיפה (10%)	2	משך גילוי התקיפה (2.0): התוקפים פעלו במשך 9 חודשים ללא זיהוי, נקודת חולשה קריטית.
מגזר מותקף (15%)	15	מגזר מותקף (15.0): פגיעה בתשתיות IT המשמשות ארגונים פיננסיים וממשלתיים בכל העולם.
פוטנציאל שיבוש (15%)	7.2	פוטנציאל השיבוש (12.0): יכולת לשבש פעילות גופים פיננסיים ישראליים שעובדים מול ארה"ב.
פוטנציאל פגיעה תשתיות כלכלית (15%)	10.4	פוטנציאל השפעה על תשתיות כלכליות (10.5): סיכון לפגיעה במערכות בנקאיות וממשלתיות בישראל.
פוטנציאל פגיעה במערכת הפיננסית (10%)	4.85	פוטנציאל פגיעה במערכת הפיננסית (8.67): חשש מגישה לא מורשית למידע פיננסי רגיש ושיבוש תהליכים.
זיקה כלכלית וגיאוגרפית (5%)	3.5	זיקה כלכלית וגיאוגרפית (5.0): קשרים כלכליים הדוקים בין ישראל לארה"ב מגבירים את פוטנציאל הפגיעה.

Colonial Pipeline - 2021

- מקור: תשתית ארה"ב
- השפעה חוצת גבולות: שיבוש אספקת דלק, שהוביל לתנודתיות בשוק
- השפעה כלכלית מחוץ למקור:
  - קנדה: מחירי הבנזין הממוצעים עלו ב-12.9% מפברואר למאי 2021, בהשפעת חששות לאספקה
  - שווקי אנרגיה גלובליים: תנודתיות מחירים לטווח קצר המשפיעה על כלכלות תלויות אנרגיה
- דווח על ידי Reuters.com

מדד	חישוב	הסבר ניקוד משוקלל
מקור (10%)	7.5	הדיווח היה מהיר ואמין יחסית עם אימות ממקורות רשמיים, אך עם מידע טכני מוגבל. 75/100
התקפה (10%)	8	מתקפת כופרה מתוחכמת שכוונה לתשתית קריטית להובלת דלק, בוצעה על ידי ארגון פשיעה מקצועי. 160/240
ארגון נתקף (10%)	8	מגזר אנרגיה עם השפעה בינונית על תשתיות ישראל, בעיקר דרך השפעות עקיפות על שווקי אנרגיה גלובליים. 80/100
משך גילוי התקיפה (10%)	10	גילוי מהיר של המתקפה (0-4 שעות) אפשר תגובה מיידית וצמצום נזקים פוטנציאליים. 50/50
מגזר מותקף (15%)	9	תאגיד ענק בתחום האנרגיה עם השפעה משמעותית באזור החוף המזרחי של ארה"ב, מוביל שוק בתחומו. 60/100
פוטנציאל שיבוש (15%)	9.5	בזמן אמת היה חשש לשיבוש משמעותי בשוק האנרגיה עם השפעות גלובליות ולתקופת התאוששות ארוכה. 70/110
פוטנציאל פגיעה תשתיות כלכלית (15%)	9.2	חשש משמעותי להשפעה על מחירי אנרגיה ותשתיות פיננסיות גלובליות הקשורות לשוק האנרגיה. 80/130
פוטנציאל פגיעה במערכת הפיננסית (10%)	4	חשש מוגבל להשפעה על המערכת הפיננסית בישראל, למעט תנודתיות אפשרית במניות אנרגיה וארגונים פיננסיים עם חשיפה לשוק זה. 130/330
זיקה כלכלית וגיאוגרפית (5%)	2.5	קשר כלכלי בינוני עם ריחוק גיאוגרפי משמעותי, המצמצם את עוצמת ההשפעה הישירה על ישראל. 50/100


איסוף ידיעות בזמן אמת
ניתוח ראשוני למידע שנסרק
סיווג אירוע?
התקפת סייבר אמיתית
לא רלוונטי
מחולל הערכת פוטנציאל ההשפעה
סיום
הערכת מאפייני האירוע
הערכת השפעה פוטנציאלית על ישראל
חישוב ציון סופי
רמת סיכון
שליחת התראות לבעלי תפקידים
דשבורד משתמש
מרכז מודיעין מאוחד
ממשק סקירת אירועים
לשונית ביצועי מודל
פונקציונליות ייצוא
Human-in-the-loop
משוב לשיפור המערכת