

Microsoft Security Bulletin Analysis

דוח פריסת מוצג על ידי בר כהן וסהר חיים יעקב.

דוח זה עוסק בשלב הפריסה של תוכאות ניתוח הנתונים בפרויקט. מטרתו היא לתאר את תהליך יישום המודלים הנבחרים במערכת, תוך התיאור של שילובם בפלטפורמות קיימות, ניתורם השוטף ותחזוקתם לאורך זמן, לשם שמירה על ביצועים מיטביים ודיקוק תוצאות בסביבה הארגונית.



שם מרצה : מר אביה זכאי.

שם מנהה : מר חנן לב.

מוגשים :

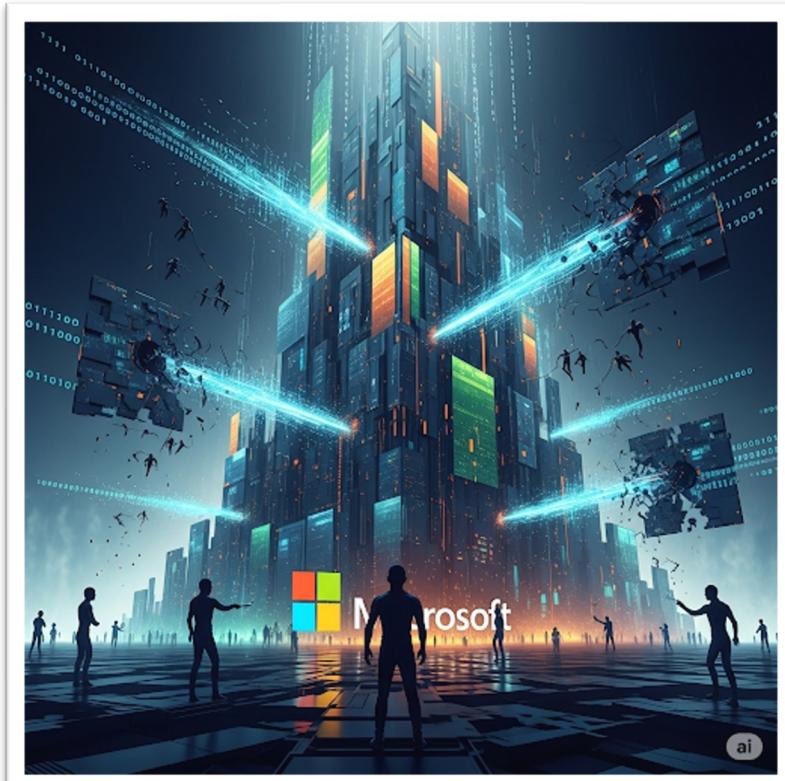
בר כהן 208110254

סהר יעקב 314741851



תוכן עניינים

- 3 -	1. תוכנית פריסה
- 4 -	GitHub 1.1
- 5 -	Tableau Public 2.1
- 6 -	MySQL 3.1
- 7 -	Gradio 4.1
3. תוכנו מעקב ותחזוקה	
- 9 -	1.2 אילו גורמים / השפעות צריכים להיות במעקב ?
- 10 -	2.2 כיצד נמדד וונטר את תוצאות ודיקח המודלים ?
- 13 -	3.2 כיצד נקבע מותי פג התוכף של כל דגם ?
- 14 -	





1. תוכנית פרישה

שלב הפרישה (Deployment) מהו זה נקודת מפנה קריטית בכל פרויקט ניתוח נתונים ולמידת מכונה. לאחר תהליכי אישור הנתונים, עיבודם, בחרית המודלים וAIMON, מגע השלב שבו התובנות והפתרונות המפותחים הופכים לנגישים ושימושיים עבור קהל היעד. פרק זה יתאר את תוכנית הפרישה המキיפה של תוכרי הפרויקט, תוך התייחסות למספר ערכוי יישום ושיטוף, אשר יבטיחו את שימוש העבודה, הצגה באופן מקצועי ויצירת ממשקים אינטראקטיביים עם המודלים שפותחו.

בפרק זה, נשלים את תוכנית הפרישה באמצעות **ביצוע הפעולות הבאות**:

שמור וניהול קוד באמצעות GitHub

בוצע העלאה מסודרת של כל מסמכיו הפרויקט, קוד המקור, וקבצים נלוויים למאגר GitHub. פעולה זו תבטיח שימור גרסאות יעיל, שקייפות היליכית, ותאפשר הצגה מפורטת של העבודה בפני גורמים רלוונטיים, תוך קידום שיתוף ידע ופוטנציאל לשיתופי פעולה עתידיים.

ניהול נתונים וחקר ב - MySQL

הנתונים המעובדים והמנוקים יועלו למסד נתונים MySQL. מסד הנתונים ישמש כמאגר נתונים מרכזיז ויציב, ויספק פלטפורמה עצמאית לניהול הנתונים ויאפשר ניתוח וחקיר מעמיק באמצעות BI שונים וניתוח נספחים שאינם Power BI, Tableau Public, לדוגמא. יכולת זו חיונית לגמישות אנליטית ולתמייה בנסיבות נתונים עתידיים.

הציג תובנות חזותיות באמצעות Tableau Public

לצורך הצגת התובנות החזותיות העיקריות הנתונות, נציג לוח מחוונים (Dashboard) אינטראקטיבי באמצעות פלטפורמת Tableau Public. הנתונים המשמשים לדashboard זה יועלו ישירות ל Tableau Public וזאת לאחר שהנתונים עברו את שלבי הניתוח והעיבוד הנדרשים. לוח המוחונים ימחיש את הממצאים המרכזיים ויאפשר למשתמשי קצה לחקור את המידע בצורה יזואלית ו互動יבית.

הגשת המודל הסופי באמצעות Gradio

נציג את תרחישי השימוש של המודל הסופי שבנוינו, אשר מtabסס על אלגוריתם CatBoost. לשם הדגמה והנגשה, נפרס את המודל באמצעות דף אינטרנט ייעודי שנבנה באופן מודולרי, תוך שימוש בספריית Gradio שביביתון. משק זה ישלב עיצוב ויוזאלי מותאים (CSS) באמצעות (CSS) ויאפשר למשתמשים אינטראקטיבית ישירה עם המודל, קבלת תוצאות והבנתו באופן פעול.

פרק זה יציג כיצד הטמעת הפתרונות הללו אינה רק סיום של תהליך הפיתוח, אלא פתח לשבד חדש שבו הערך העסקי והתפעולי של הפרויקט ממומש במלואו.



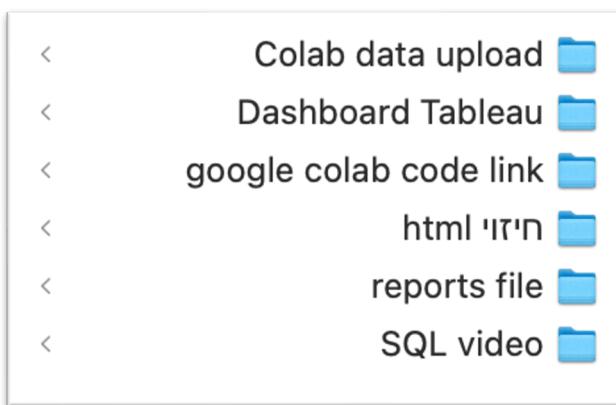


GitHub 1.1



כדי שהמודול ונתוני הדוחות ישמרו לארוך זמן ויהיו זמינים ותקפים אנו נctrarף לפלטפורמת GitHub על מנת שנוכל להעלות בה את מסמכי הפרויקט. GitHub היא הפלטפורמה האידיאלית לכך, היא מאפשרת שמירה ונגבי עם שיתוף פעולה בין צוותים, **הציגת הפרויקט לקהל מקצועי או אקדמי**, ותיעוד תהליכי העבודה באופן מסודר ונגיש. בנוסף דרכ GitHub ניתן למשוך את המודול לצורך ניסוי וסקירה וגם הטמעה לאותן החברות שיצטרכו מודלים אלו.

- **שמירה וגיבוי בענן** – כל שינוי נשמר ומוגבה אוטומטית, עם אפשרות לשחזור גרסאות קודמות.
 - **שיתוף פעולה בין חברי הצוות** – כל חבר צוות יכול לגשת לתוכו, להציג שינויים, לפתור קונפליקטים ולעבוד בסyncron מלא.
 - **תיעוד מקצועי** – ניתן לתעד את תהליכי העבודה בצורה מסודרת.
 - **חשיפה לקהל מקצועי** – אנשי מקצועי, חוקרים, או מראיניים פוטנציאליים יכולים להתרשם מהפרויקט ומהיכולות הטכניות והמתודולוגיות של הצוות.
 - **סטנדרט בתעשייה** – שימוש בGit ובפלטפורמות כמו GitHub הוא חלק בלתי נפרד מתחליני הפיתוח בתעשייה ההיטק. שילוב של Git בפרויקטים אקדמיים מדמה סביבת עבודה אמיתי, ומakin את חברי הצוות לעובדה בצוותי פיתוח מקצועיים, תוך שימוש ב- Branches, Pull Requests, Code Reviews
- כדי להעלות את המסמכים בצורה מסודרת אנו ניצור תיקיות כדי לאחסן כל קובץ בנפרד למשל -
בתוך כל תיקיה נאחסן את המסמכים הרלוונטיים.



בנוסף לשמירה גיבוי והציגה של מסמכי הפרויקט, GitHub תורם להרחבת עתידית, שיקיפות תהליכי כמו מעקב ברור ושיתוף פעולה על סמך קוד פתוח.

לxicom GitHub, הוא הרבה מעבר למקומות אחסון: הוא תשתיית שלמה לניהול ידע, תהליכי, שיתוף פעולה ומקצועיות, והוא מעניק לפרויקט יתרון אמיתי – גם בטוחה הקצר של ההגשה, וגם בטוחה הארוך של יישום עתידי בעולם האקדמי או העסקי.

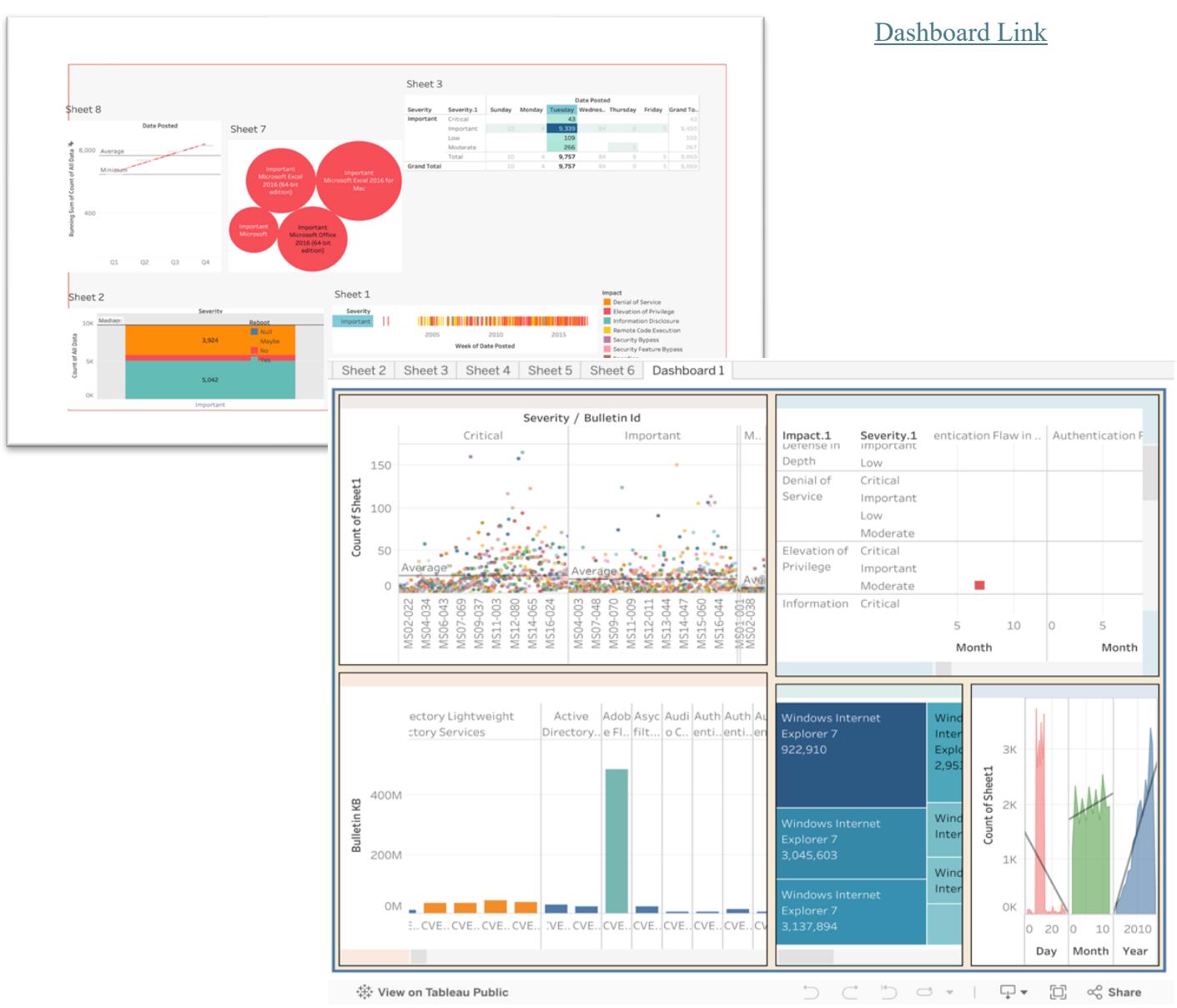


Tableau Public 2.1



כדי להמחיש את הנתונים שהורדנו מאתר Microsoft , הכנו ב - Tableau Dashboard מותאמת לנתחים. כדי להמחיש בצורה ויזואלית את הנתונים והמשמעות שלהם יצרנו גרפים שונים , עמודות , קווים , טבלאות ועוד . בתמונה מתוך ה - Dashboard יש לנו ראות צילום מסך חלקו ובו חילוק הנתונים לפי ימים , וסוגי התקיפה . בצילומים המסך סיננו את התקיפות ליום שלישי וסוג התקיפה מסווג - Important . ניתן לראות את הכליה בה בוצע התקיפה - מניעת שירות , העלאת הרשות , חטיבת מידע , הרצת קוד מרוחק , עקיפת אבטחה , עקיפת תוכנות אבטחה , זיווג , וערכה בלתי מורשתית . בנוסף ניתן לראות את כמות התקיפות שבוצעו ביום זהה , ממויצת התקיפות , מגמות התקיפות ועוד . ניתן לומר שביום שלישי בוצעו רוב התקיפות כ - 9,757 , מסוג Important . ניתן להסביר כי יום שלישי הוא היום בו Microsoft נמצא בסכנה מפני רוב התקיפות ולכןណ לנצח את רוב המשאים על יום שלישי . בגרף הגודל של העיגולים , הגודל מצין את כמות התקיפות וגם ניתן לראות מאיזה סוג מערכת הפעלה בוצעה התקיפה , כולל - mac/windows . צילום המסך הוא מתוך תחילה הכתנת ה - Dashboard ולא התוצר המוגמר .

[Dashboard Link](#)





MySQL 3.1

בחרנו לעלות את הנתונים שלנו לתוכה מסד נתונים MySQL, באמצעות קוד פיתון. כדי להתmeshק צריך פרטיה הزادות, הקמו מסד נתונים הפיתון בשם project_database ושם הטבלה שבחרנו Microsoft_Attack, בנוסף הוספנו מפתח ID מתוך הפיתון אם לא קיים והצלחנו להריץ שאילתות פשוטות יחסית.

הקוד פועל על התוכנה באופן מקומי ישירות על מחשב האיש, ללא צורך בהתקשרות עם שרת או ענן חיצוניים. גישה זו מאפשרת שמירה מירבית על פרטיות הנתונים, מהירות תגובה גבוהה יותר, ושליטה מלאה על סביבת העבודה. כמו כן, עבודה מקומית מבטיחה עצמאות מרשות תקשורת ומפחיתה סיכון.

הנתונים שהורדנו אינם מכילים את עמודות ה - ID, היא נוספה לשם מפתח ייחודי של כל תקיפה. באמצעות SQL – הרצינו שאילתות מתקדמות יותר, כלי העור הזה מאפשר לנו לשנן ולמצוא פרטיים חשובים על הנתונים (סינון מתקדם יותר).
לפי צילום המסך אנחנו בוחרים בעמודות id, הרכיב שהושפע, שיחזור, סיווג ראשוני ומשני של התקיפה. בוחרים מתחם הטבלה בשם חלופי ma (Microsoft_Attack), כדי לפשט את התהילה.
מתוך שורות אלה סיננו את הרכיבים של windows ו- mac שמכילים את המספר 16, לבסוף סידרנו את הנתונים לפי סדר אלפביתית יורץ מהסוף להתחלה לפי משתנה המטרה - Severity (A-Z).

ערכנו השוואה בין windows ו- mac – מחשבים הפעלה מחדש עדכון לעומת Windows שכן צריכים הפעלה חדשה, בעוד סינון ניתן לראות כי מרבית התקיפות של Windows קריטיות בסיווג הראשוני ובמשני לעומת Mac שנחשבות חלשות, אפשר להסיק מכון רמת האבטחה ותחזוקת המערכות השונות.

באופן כללי, השימוש ב-SQL מאפשר לנו לנחל את הנתונים בצורה חכמה ומדויקת, להוציא מהם תובנות אינטואיטיביות ולהיעיל את תהליך העבודה עם מאגרי מידע מורכבים.

למה SQL?

SQL ישן שאילותות שמאפשרות מיקווד וסינון נתונים בצורה מדויקת ומהירה, מה שחווסף זמן רב בעבודה עם כמות גדולה של מידע (כמו בפרויקט זה). במקום לעבור על כל הרשומות באמצעות כלים פשוטים ולא ייעלים, ניתן לכתוב שאילתת שתחלץ בדיקות המידעד הרלוונטי בלבד.

בנוסף SQL, תומכת בפעולות חישוביות וכליות שמאפשרות לבצע סיכומים, ממוצעים, ספירות ועוד, כך ניתן לקבל דוחות ונתחומים סטטיסטיים בצורה קלה ומהירה. פעולות אלו מאפשרות ליזמות מגמות, חיריגות ודפוסים בתוצאות במהירות, ומספרות את איקות הניתוח העסקי והמחקר. SQL נחשבת לשפה עצמאית מאוד עם יכולות מורכבות לביצוע חישובים, סינונים, מיזוג טבלאות, חישובים ודוחות, בעוד שמערכות ניהול נתונים אחרות, כמו NoSQL, מתמקדות בגימות מבנית ולא תומכות בשאלות מורכבות ברמת הייעילות.

בנוסף כל SQL הוא בחירה מותאמת עבור מחקר של מידת מכונה ולצורך זאת אנסט.

The screenshot shows the MySQL Workbench interface. The top navigation bar includes tabs for 'Administration' and 'Schemas'. The main area has a 'Query 1' tab open, displaying the following SQL code:

```

SELECT ma.ID, ma.Affected_Component, ma.Reboot, ma.Severity
FROM Microsoft_Attack ma
WHERE
    ma.Reboot IN ('Yes', 'No')
    AND ((ma.Affected_Component LIKE '%Mac%' AND ma.Affected_Component LIKE '%16%')
    OR (ma.Affected_Component LIKE '%Windows%' AND ma.Affected_Component LIKE '%16%'))
ORDER BY ma.Severity desc

```

Below the code, the 'Result Grid' pane displays the following data:

ID	Affected_Component	Reboot	SeverityPOINT1	Severity
4026	Microsoft Excel 2016 for Mac	No	Important	Important
4537	Microsoft Excel 2016 for Mac	No	Important	Important
300	Windows 10 Version 1607 for 32-bit Systems	Yes	Critical	Critical
304	Windows 10 Version 1607 for x64-based Systems	Yes	Critical	Critical
308	Windows Server 2016 for x64-based Systems	Yes	Moderate	Critical
370	Windows 10 Version 1607 for 32-bit Systems	Yes	Critical	Critical
373	Windows 10 Version 1607 for x64-based Systems	Yes	Critical	Critical
376	Windows Server 2016 for x64-based Systems	Yes	Moderate	Critical



Gradio 4.1

כדי להמיץ את תוצאת המודל CatBoost בניתוח הנתונים, פיתחנו כלי אינטראקטיבי בפייטון באמצעות Gradio (ייצור דף אינטרנט), המאפשר חיזוי רמת הסיכון של רמת האבטחה במוצר מיקרוסופט.

באמצעות פלטפורמת Gradio ניתן לבנות ממשק אינטרנט HTML מתוך Python באמצעות ספריית Dash, מכילה רכיבים שיכולים לבנות אתר אינטרנט כמו Html וגם עיצוב חיצוני/פנימי מתאים.

ספרייה Dash

Dash היא ספריה שנitizen ליצור באמצעות יישומים אטרקטיביים בצורה קלה, שימושה העיקרי הוא בתחום ניתוח הנתונים, למידת מכונה, מדעי נתונים ויזואלייזציה. יתרון הבולט של הספרייה הוא שאין צורך בידע קודם ב-HTML, CSS או JavaScript.

: *ישנם מספר יתרונותבולטים לשימוש ב-Dash*

- קוד נקי, באמצעות python בלבד.
- מותאם למידול נתונים וגם ללמידה מכונה.
- הרצה מקומית או על שרת ענן – لكن יש צורך להריץ את הקוד מחדש בכל פעם.

GRADIO	DASH	תכונה
מודלי python בסיסי הדגומות מהירות ונוחות	ויזואלייזציה וdashboards Python\html\css Css + bootstrap אפליקציות מורכבות	מטרה שפות עיצוב התאמה

בחרנו בDash ו-Gradio כי ניתן לכתוב בשפת פייטון ולא לערबב גרסאות שונות של הפרויקט.

בדוגמא זו הקוד הוא מודולרי ולא עבר תכונות ספציפיות, הפרמטרים הם רשימת התכונות ורשימת האפשרויות הייחודיים מתוך כל עמודה.

ניתן לבחור את התכונות והפרמטרים המתאימים ע"י לחיצה ולקבל משוב, התכונות (תכונות המודול) הם :

.1 **Impact: Elevation of Privilege** השפעת הפגיעה שנבחרה היא העלאת הרשות. המשמעות היא שהтокף יוכל, באמצעות ניצול הפגיעה, להשיג רמות גישה גבוהות יותר במערכת מאשר לו במקור, לדוגמה משתמש רגיל למנהל מערכת.

.2 **Title: Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution** כוורת הפגיעה מתארת בעיות אבטחה.

.3 **Severity: 1: Moderate** חמורת הפגיעה ראשונית סוגה כ"בינונית".

.4 **Supersedes: MS08-035 (940214)** עדכון אבטחה שמחילף או מבטל עדכונים קודמים תחת הקוד.



Reboot: Yes .5

האם יידרש אתחול (הפעלה מחדש) של המערכת לאחר יישום התיקון לפגיעה זו, על מנת שהשינויים ייכנסו לתוקף באופן מלא.

CVEs: CVE-2008-1456, CVE-2008-1457 .6 מוחה ייחודיים.

Affected Component: Microsoft Windows Messenger 4.7 .7 הרכיב המושפע.

Component KB: 956380 .8 מידע נוסף ופרטים טכניים.

לאחר בחירת הפרמטרים מתוך הרשימות שהגדנו, נרים את המודל ותוצאת המודל היא, שהתקיפה חשובה.
כלי זה ממחיש כיצד ניתן להשתמש בפייטון וב- Gradio לבניית יישומים אינטראקטיביים המאפשרים למשתמשים לחקור ולנתה נתונים בצורה נוחה ודינמית.

```
def run_dashboard(features , save_label): 1 usage
    dropbacks = []

    for i, feature in enumerate(features):
        dropbacks.append(
            html.Div( children: [
                html.Label(feature),
                dcc.Dropdown(
                    id={"type": "dropdown", "index": i},
                    value=save_label[i][0]['value'],
                    options=save_label[i],
                    placeholder=f"choose {feature}",
                    className="form-control"
                )
            ], style={"margin-bottom": "10px",})
        )

    app.layout = html.Div([
        html.H2( children: "Prediction Microsoft Security", className="text-center mb-4"),
        html.Div(dropbacks, className="container"),
        html.Button( children: "Send", id="submit-button", className="btn btn-primary mt-3"),

        html.Div(id="output-container", className="mt-4"),
        html.Div(id="output-model-result", className="mt-4")
    ])

```

תצוגה מתוך הדף שיצרנו.

Prediction Microsoft Security

Please choose options from the dropdown menus and press 'Send' to receive the model's prediction.

Impact	Elevation of Privilege
Title	Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution
Severity	Moderate
Supersedes	MS08-035/949014
Reboot	Yes
CVEs	CVE-2008-1456,CVE-2008-1457
Affected Component	Microsoft Windows Messenger 4.7
Component KB	956380

Flag

output
Model Prediction: ['Important']

Clear Submit



2. תכנון מעקב ותחזוקה

בפרק זה, נתמקד בשלבי הסיום הكريティים של הפרויקט, הכוללים תוכנית מפורטת למעקב שוטף, ניטור ביצועי המודלים, ותחזוקה אקטיבית לאורך זמן. מטרת slab הפרסה אינה מסתכמה רק בישום המודלים, אלא כוללת גם הבטחה שביצועיהם ישארו אופטימליים, מדויקים וROLONNTIIMIS בסביבה הארגונית המשתנה. תעוזד ושיתוף התוצרים בפלטפורמות מקצועיות, כפי שפורט בפרק 1, הינס חלק בלתי נפרד מתהיליך זה, שכן הם מאפשרים שקיפות, שיתוף פעולה והמשכיות.

מבוא לניהור ותחזוקה: הקשר לניטויי עדכוני אבטחה של Microsoft

קובץ הנתונים שברשותנו מתאר עדכוני אבטחה שהופצו בעבר רכבי תוכנה מגוונים במערכות הפעלה של Microsoft. כל רשומה בקובץ מספקת מידע מודיען אודות עדכון ספציפי, ובכלל זה מזהה העדכון (Bulletin ID), קוד בסיס המידע (KB) הנלווה אליו, דרגת חומרת הפגיעה (Affected Product), השפעתה הפוטנציאלית (Impact), מערכות ההפעלה המושפעות (Severity) – לרבות 10 Windows 7, 8.1, וגרסאות שונות של Windows Server – וכן את רכיב התוכנה או החומרה הפוגע (Affected Component). בנוסף, הנתונים כוללים אינדייקציה האם העדכון מחייב הפעלה חדשה של המערכת (Reboot), וקישורים למזהה פגיעויות בינהו (CVE). חשוב לציין כי רוב העדכנים מתייחסים לפגיעות קרייטיות כגון "Remote Code Execution" (ביצוע קוד מרוחק), אשר עלולות לאפשר לתוכפים להציג גישה בלתי מורשית למערכת.

ניתוח עמוק של נתונים אלו חיוני להבנת דפוסי עדכוני האבטחה של Microsoft ולזיהוי הפגיעויות המשמעותיות ביותר במערכות הפעלה וברכבי תוכנה מגוונים. חשיבותו של ניתוח נתונים מסווג זה, ואיתו הצורך במערך מעקב ותחזוקה חזק, נובעת מספר יתרונות אסטרטגיים ותפעוליים:

- מניעת התקפות אבטחה:** פגיעות קרייטיות המפורטו בעדכנים, דוגמת "Remote Code Execution", מהוות סיכון ממשוני למערכות ולארגוני. ניתוח הנתונים מאפשר זיהוי מהיר של העדכנים בעלי החשיבות הגבוהה ביותר ותעדוף יישום. לצורך זה, מערכת מעקב ותחזוקה אקטיבי היא המפתח לצמצום חלון החשיפה לפגיעה.
- SHIPOR מדיניות האבטחה הארגונית:** באמצעות ניתוח מתמיד של הפגיעויות ותגובה מהירה לתיקון, ארגונים יכולים לשפר באופן אקטיבי את מדיניות האבטחה שלהם. גישה פרואקטיבית זו, המוגבה במנגנון ניטור ותחזוקה, מסייעת במניעת נזקים עתידיים, לרבות אובדן נתונים, פגעה במוניטין והשלכות כספיות, הנובעים מפגיעויות בלתי מטופלות.
- זיהוי מגמות ואיתור סיכונים מפותחים:** ניתוח כמותי של הנתונים מאפשר לחוש מגמות אבטחתיות מפותחות, כגון עלייה בתדרות או בסוג הפגיעויות בתחום ספציפי לאורך זמן. תובנות אלו חיוניות למיקוד עיל של משאבי אבטחה, לפיתוח אסטרטגיות הגנה ממוקדמות, ולהיערכות לאיומים חדשים – וכל זאת מחיבר מערכות ניטור מתמשכות.
- ת邏MICHAה בדרישות תיעוד ו齊יות (Compliance):** עבור חברות וארגוני גדולים, ניתוח ווישום מוסדר של עדכוני אבטחה הם חלק בלתי נפרד מדרישות רגולטוריות ו מדיניות ציונות פניות. המידע המתתקבל משמש כתיעוד מהימן וחיווני עבור ביקורות פניות ודווחות רגולטוריים, ובבטייח עמידה בתקני אבטחה מיידע מחמירים – תוצר לוואי הכרחי של תהליכי תחזוקה מוקפם.

לסיכום, ניתוח זה מעניק למומחי אבטחה תמונה בהירה, מפורטת וארוגנית גודלים, ניתוח האבטחה של המערכות בארגון. הוא מהווה את הבסיס האנליטי לעליון נבנה תכנון המערכת והתחזוקה בפרק זה, אשר חיוני לשמרה על סביבת מידע מוגנת ומעודכנת באופן שוטף.



1.2 אילו גורמים / השפעות צריכים להיות במעקב ?

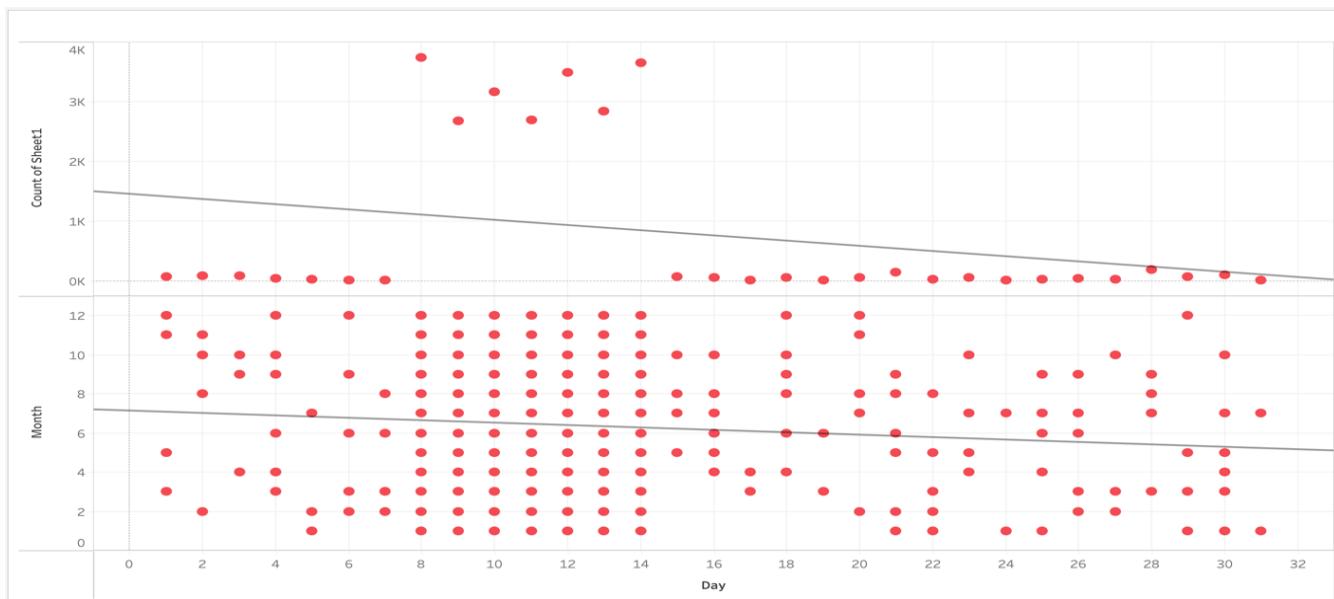
בדאטה שלנו יש הרבה מילים שנרצה להיות במעקב אחריהם, כגון : Severity.1, Severity, Impact.1, Impact CVEs, ... ועוד ... נזכיר את ניתוח מאפייני הנתונים שדוחות הקודמים לשם סקירה וסבירו התכונות עליהם נבצע את המיעקב -

שם תכונה	הגדרה	תיאור
Date Posted	The date when the bulletin was published.	מצין מתי עדכן האבטחה או העלו שוחררו באופן רשמי.
Bulletin Id	The unique identifier for the security bulletin.	עזרה בהפניה וטווית דוחנו באמצעותו.
Bulletin KB	Knowledge Base (KB) number associated with the bulletin.	-links לDocumentation טכנית מפורטת על update.
Severity	The criticality level of the update.	Defines the importance of applying the update, such as Critical, Important, etc.
Impact	The type of vulnerability the update addresses.	Specifies whether the vulnerability impacts Remote Code Execution, Denial of Service, etc.
Title	The title of the security bulletin or update.	Provides a brief description of the update or its purpose.
Affected Product	The product impacted by the vulnerability.	Lists the operating systems, applications, or services requiring the update.
Component KB	The Knowledge Base (KB) number for the affected component.	Specifies the technical documentation for the impacted component.
Affected Component	The specific component affected by the vulnerability.	Details the part of the product or service that is vulnerable.
Impact.1	Secondary impact description for the vulnerability.	Further clarifies the vulnerability's effect, if needed.
Severity.1	Secondary severity level for the update.	Provides an additional severity classification, if applicable.
Supersedes	The bulletin or update that this one replaces.	Indicates updates that are deprecated or no longer applicable.
Reboot	Whether a reboot is required after applying the update.	Indicates if the system needs to restart to complete the update installation.
CVEs	Common Vulnerabilities and Exposures identifiers.	Lists standardized IDs for vulnerabilities addressed by the update.

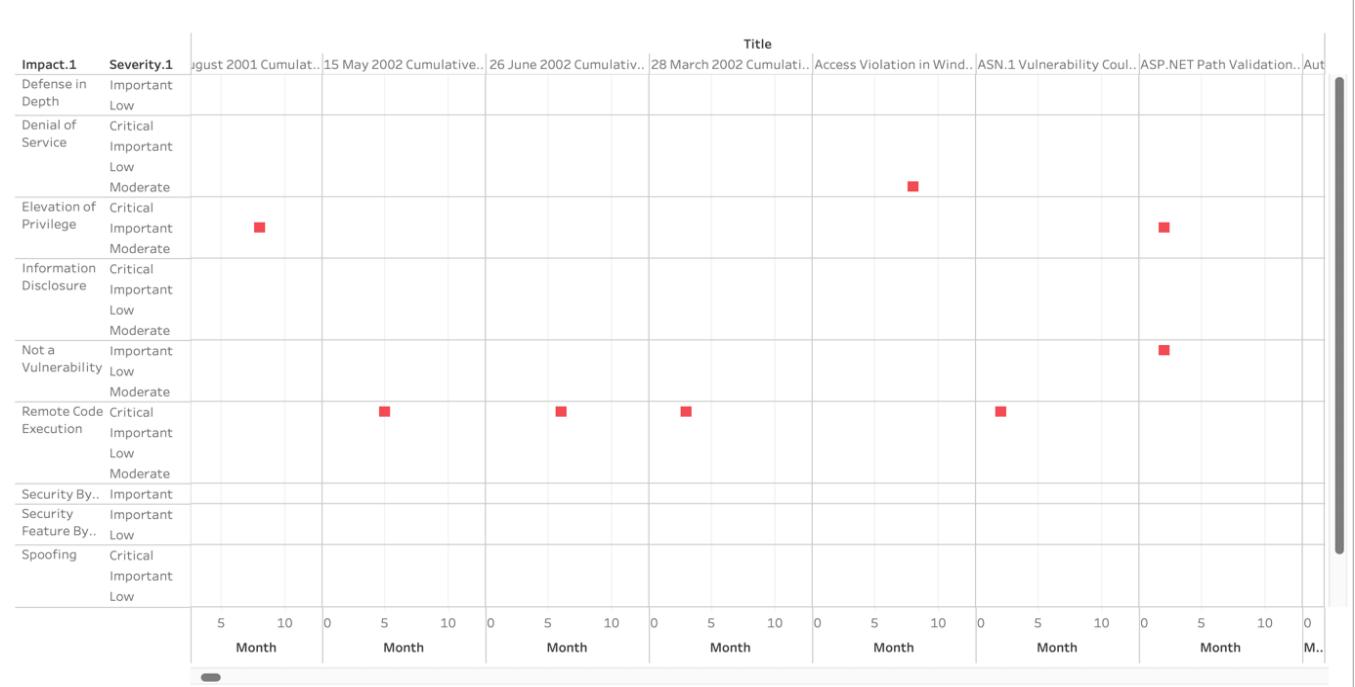
שם תכונה	הגדרה	תיאור
תאריך פרסום	התאריך שבו פורסם הuletton.	מצין מתי עדכן האבטחה או העלו שוחררו באופן רשמי.
זהה לעליון	זההה הייחודי של דוחנו באמצעותו.	עזרה בהפניה וטווית דוחנו באמצעותו.
KB עליה	מספר מאגר הדעת (KB) המשויך לדוחנו.	קישורים לתשען סכני מפורט על העדכנים.
חומרה	רמת קיטוריות של הדוחן.	נדיר תא חומרה של דוחן כדוגמת קרטיסי, חשב וכו'.
פניות	סוג הפגיעה שבה הדוחן מסוף.	מצין אם הפגיעה מסוימת עלייה ביצוע קוד מרחוק, מניעת שירות וכו'.
ונקודות	הכוורת לשעון אבטחה או הדוחן.	מספק איזור קרע לשעון או טסתה.
מודול מושפע	המודול שהושפע מפגיעה.	מפורט תא בערכות הhardware היישומיים או השרתויים הדוחשים עדכנים.
KB ריבכין	מספר מאגר הדעת (KB) עבור הריבכין המושפע.	מצין את התיקוד הנקני עבור הריבכין המושפע.
ריבכין מושפע	הריבכין מסווג הושפע מהפגיעה.	פרוטת חקל של המזוז או שירותי פפיין.
השפעה.1	תיאור הפגיעה מוגברת לעומת הפגיעה.	ambilhar עוז יזרעאל השפעה הפיפוי, במידת הצורך.
1. מוגראת.1	רמת חמירה מסוימת בעור הדוחן.	מספק סיווג חמירה ופאיין, אם רלוונטי.
מחלף	העלון או הדוחן שאחדח חזר מחלף.	מצין עדכונים שיאו משמש או אינם שימושיים עוד.
אלתית CVEs	אם דרוש אלתית מודול לשערת הלהת העדכנים.	מיין אם המעכנת צריכה לפעוף מודול דוד להלאת את התקנת העדכנים.
		מספר מודלים סטנדרטים עבר-גנוקוּנט טעינה המטופלית על ידי העדכנים.

כפי שניתן לראות, יש לנו הרבה תכונות קריטיות שהיינו רוצחים לבצע עליהם מאחר וכל תכונה היא רלוונטית ויכולת להוועיל לנו בתובנות ומיציאת קשרים בהמשך לצורך חיזוי התקפות עתידיות. לצורך העניין אם יש לנו תכונה מסווג כAffected Product או כAffected Component היינו רוצחים לדעת מה רמת הפגיעה שחוות או איזה ריבכין או מודול/שירות נפגע שכן אם נתקב וננטור לוגים אלה נוכל להגיע למסקנה שאכן יש חולשה באותה שירות או ריבכין. נוכל ללמוד את המודל מתי, כמה ואיפה ע"פ מעקב וניתוחים אילו מהי תקיפה וסיכון ממשי ומהו רישום לוג תקין במערכת.

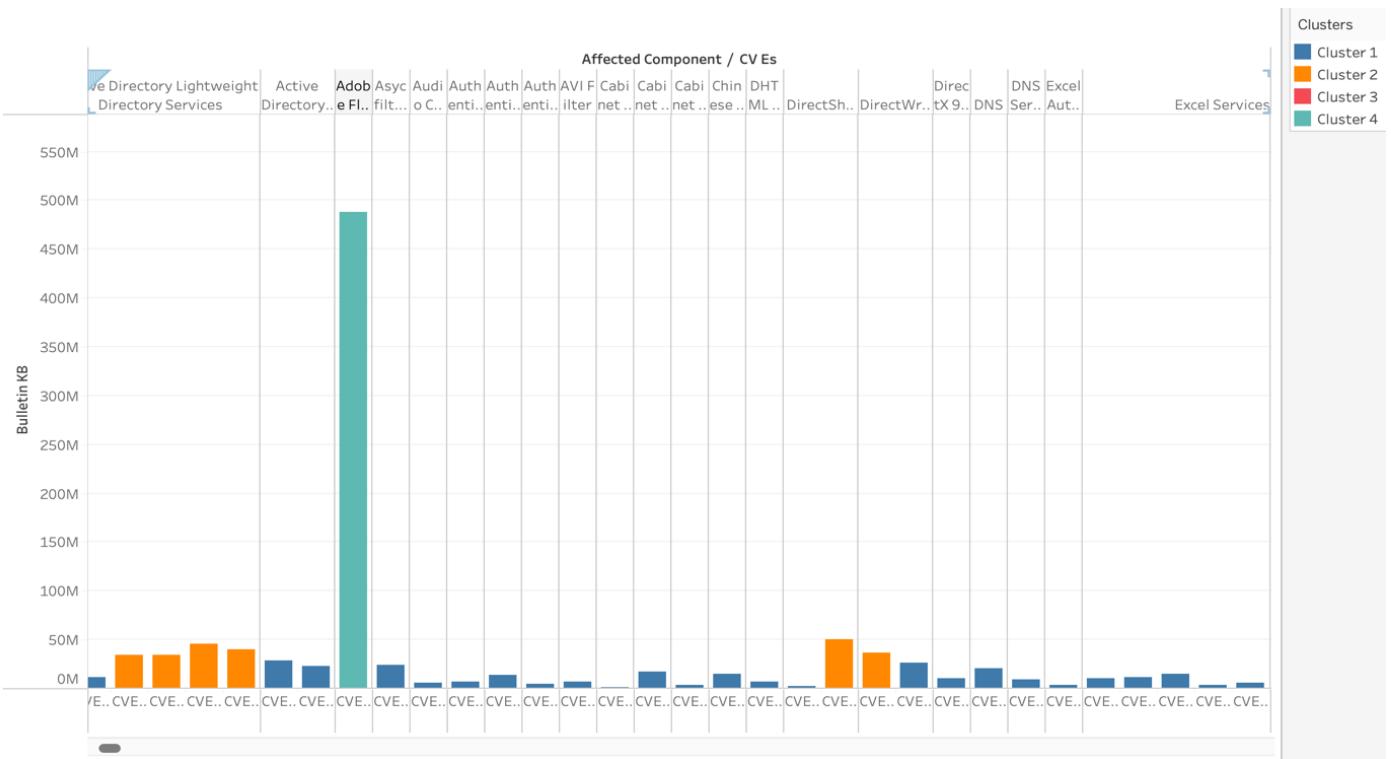
כלומר נרצה לחבר לאלגוריתם שלנו מערכת רישום (SIEM – Security Information and Event Management) מותך אותה החברה שתהיה מעוניינת בכך, ובכך למד את המודל בצורה richtig את הרישומים השונים שנמצאים במערכת. נראה כמה גורפים על הדאטה שלנו מתוך Tableau אשר מראים כיצד היינו מנתחים, וכיצד היינו שמים לב לאותם הלוגים הרישומים במערכת החברה.



- ניתן לראות שימים 8 עד 14 הותקפו/ביצעו עדכוניים לאורך כל החודשים. בנוסף ניתן לראות שאלו הימים לאורך החודשים שהו הכי הרבה רישומי לוג חריגים כבין 2600 ל 3700 (בנים התקפות ועדכוניים).



- בגרף זה ניתן לראות את כוורות הלוג מסוירות ע"פ חודשים לצד השפעות שבתוכם יש סיווג לרמת הקriticיות של אותה השפעה מנומכה לkriticit. ככל מרע ע"פ גרף זה ניתן לדעת וללמוד את המודל מהי בעיה קritisית ומהי בעיה נמנכה ולפי זה נוכל ללמוד אותו לחזות עדכוניים או מטרות שנרצה למש ובקൾ למנוע התקפות עתידיות – בכך שמננע חולשות. לצורך העניין בגרף זה ניתן לראות התקפה מסווג Elevation of Privilege (סוג התקפה שבה התקוף מקבל הרשות גבואה יותר ממה שהוא רשום) המשוגגת כחשובה. בנוסף יש עוד המונח התקפות שנוכל למצוא אשר רשומות בגרף זה כמו הידוצה Remote Code Execution ו- DDOS.



- בגרף זה ניתן לראות שירות שנפגע באופן קשה מאוד, המיויחס לו ככמעט חצי מיליון מידעים שנפגעו מאותו שירות זה, השירות הוא Adobe Flash Player, אשר היה תוסף לדפדפים השונים והיה יעד אסטרטגי לאקרים בשל פרצות רבות לאותו השירות.



2.2 כיצד נמדד וונטר את תוצאות דיווק המודלים ?

עבור כל ממצא נציג את הרכיבים ותכונות המעקב כמו שווי שוק או עונתיות. כיצד נמדד ואיך נרתקפות ודיוק מודלים ונקבע האם יש מצב בו תוקפו של המודל פג או שינויים צפויים של הנתונים למשל האם המודל שבנו יהיה רלוונטי לאורך זמן – ימים, חודשים, שנים ? – מה טווח זמן הרלוונטיות של המודל ?

למדידה וניתור של תוצאות דיווק מודלים, משתמש במדדים כמותיים איקוטיים בהתאם לסוג המודל.

בנוסף נשלב כלי ניטור כדי לוודא שהתוצאות נשמרו גם לאורך זמן.

כדי למדד את תוצאות דיווק המודלים השתמש במדדים כמותיים :

דיווק המודל – אחוז התוצאות הנכונות מכל התוצאות.

Precision – מדדים לזיהוי של נתונים לא מאוזנים.

Recall – משלב את Recall ו-Precision לממד אחד מאוזן.

Confusion Matrix – טבלת שימושת את סוג הטעויות שהמודל מבצע, עורך השוואת בין תוצאות המודל לתוצאות האמיתיות של הנתונים.

עבור כל ממד נציג את היתרונות, החסרונות ואיך נמדד בצורה אופטימלית.

מדד אופטימלית	חסרון	יתרון	
ኒקיי נתונים ומדדים של חוסר איזון.	לא מבחין בין סוגי הטעויות	טוב לנواتים עם מחלקות מאוזנות	Accuracy
Recall עם איזון ובפרמטרים ובצורה נכונה של המודל	חומר איזון בניבוי אופטימי של המודל	חשוב כאשר שגיאת המודל גבוהה	Precision
Precision עם שילוב F, שימוש בנתונים מגוונים.	עלול להוביל לעלייה בשגיאות הניבוי	חשוב למניעת false-negatives	Recall
שילוב ממדדים נומפיים, ומניעת הטיה.	אין פירוט מלא על הטעויות.	ממוצע הרמוני מאוזן בין Precision ו-Recall	F1 Score



בדי לנטר את התוצאות של המודלים נשתמש בשיטות שונות:

יתרונות	חסרון	מדידה אופטימלית
זיהוי ירידת מוקדמת במציאות והתאמת המודל בזמן	דורש מעקב רציף	השואפת ביצועים על נתונים חדשים ומידיה תקופתית.
ויזואלייזציה של תוצאות	יכול להסתמך על פרשנות אישית	גישה מידע ברור וainmentואיטיבי על ביצועי המודל Dashboard
NEYTOR SHINNOIMIM בנתונים	זיהוי מורכב ודורש משאבים	שימוש בכלים סטטיסטיים ליזיהוי דיפרנציאציה בנתונים ומטען התראה אוטומטית
ניסויים מבוקרים	ברירה מותאמת בין גרסאות	ניסוי מבוקר ובחינת ביצועים סטטיסטיים
איסוף ומשוב משתמשים	לא מייצג את כלל המשתמשים, יכול להיות סובייקטיבי	איסוף משוב באופן שיתתי וקבוע,
התראות	סיכון להתראות שגויות	הגדרת סף רגישות מתאים והתאמת מערכת ההתראות לאורך זמן

3.2 כיצד נקבע מתי פג התקוף של כל דגם ?

קביעת פג התקוף של המודל מתבצעת על בסיס של ניטור ביצועים, זיהוי שינוי בנתונים, והערכה של תקופת זמן.

מעקב ביצועים לאורך זמן - נבדוק את ביצועי המודל על **נתונים חדשים לאורך זמן**.

אם המודדים יורדים מתחת לסקן קבע, אז המודל כבר פג וצריך לעדכן אותו או להחליפו.

זיהוי שינוי בנתונים - אם התפלגות התכונות שהמודל מקבל משתנה, ביצועיו של המודל יפחתו.

שינויים אלו יכולים להתרחש בעקבות, טrndים, זמן או שינויים חיצוניים.

גילוי שינויים באמצעות ML יכול להפעיל התראה על פג התקוף.

הגדרת תקופת התקוף מראש - נוכל להגיד מראש טוחן זמן בו המודל יהיה רלוונטי לדגם, כמו :

שנתיים – במודלים שפועלים בסביבה יציבה מאוד יכול להאריך את זמן הרלוונטיות אך חשוב לדעת מתי פג התקוף.

חדשניים – מודלים של שווים משתנים או בסביבות דינמיות.

טrndים – תקופת התקוף עשויה להיות קצרה מאוד, בהתאם לעלייה וירידה של טrndים.

