

# 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 :

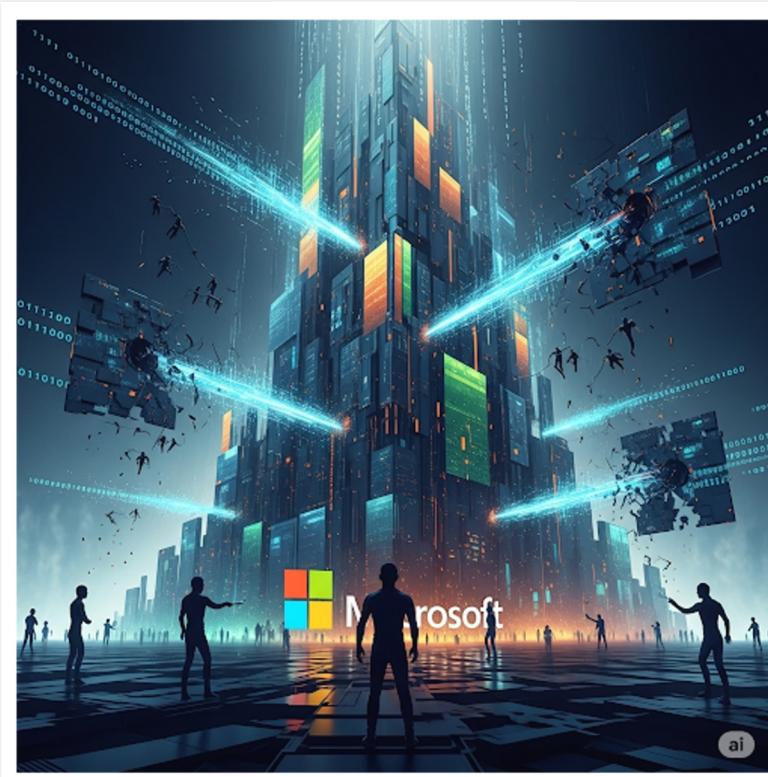
בר כהן 208110254

סהר יעקב 314741851



## תוכן עניינים

- 3 -	1. תוכנית פרישה
- 4 -	GitHub 1.1
- 5 -	Tableau Public 2.1
- 6 -	MySQL 3.1
- 7 -	Gradio 4.1
- 9 -	Hugging Face Spaces 5.1
- 10 -	2. תכנון מעקב ותחזקה
- 11 -	2.1 אילו גורמים / השפעות צריכים להיות במעקב ?
- 14 -	2.2 כיצד נמדד וננطر את תוצאות ודיוק המודלים ?
- 15 -	3.2 כיצד נקבע מותי פג התוקף של כל דגם ?
- 16 -	קישורים





## 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

בצע הعلاה מסודרת של כל מסמכיו הפרויקט, קוד המקור, וקבצים נוספים 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 לדשבורד 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 לשלב חדש שבו הערך העסקי והתפעולי של הפרויקט ממומש במלואו.





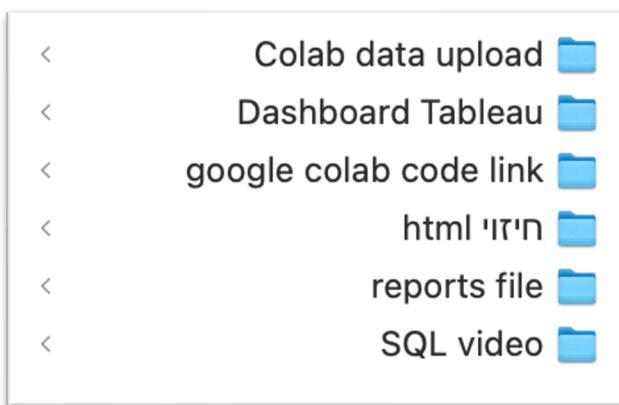
## GitHub 1.1



כדי שהמודול ונתוני הדוחות ישמרו לאורך 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 ניתן למשוך את המודול לצורך ניסוי וסקירה וגם הטמעה לאותן החברות שיצטרכו מודלים אלו.

- **שמירה וגיבוי בענן** – כל שינויים נשמר ומוגבה אוטומטיות, 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 ההייטק. שימוש 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 - ב頓ך כל תיקיה נאחסן את המסמכים הרלוונטיים.



בנוסף לשימירה גיבוי והציגה של מסמכי הפרויקט, GitHub תורם להרחבת עתידית, שկיפות תחילה כמו מעקב ברור ושיתוף פעולה על סמך קוד פתוח.

לxicoms GitHub, הוא הרבה מעבר למקום 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.

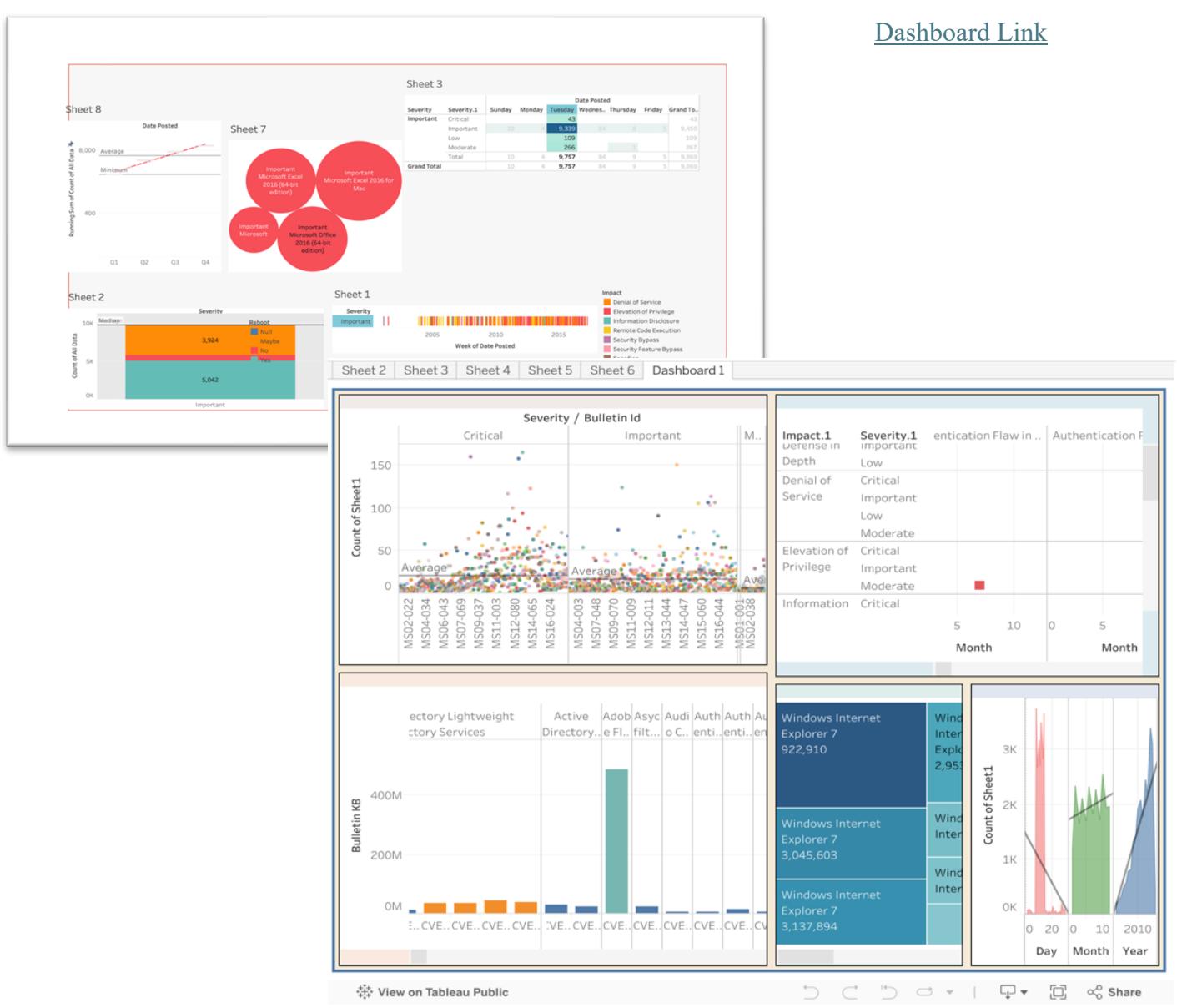


## Tableau Public 2.1



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 שצגנו ניתן לראות צילום מסך חלקו ובו חילוק הנתונים לפי ימים , וסוגי התקיפה . בצלום המסך סיננו את התקיפות ליום שלישי וסוג התקיפה מסווג - Important . ניתן לראות את הכליה בה בוצע התקיפה - מניעת שירות , העלאת הרשות , חשיפת מידע , הרצת קוד מרוחק , עקיפת אבטחה , עקיפת תוכנות אבטחה , זיווג , ועריכה בלתי מורשית . בנוסף ניתן לראות את כמות התקיפות שבוצעו ביום זהה , ממוצע התקיפות , מגמות התקיפות ועוד . ניתן לומר שביום שלישי בוצעו רוב התקיפות כ - 9,757 , סוג Important . ניתן להסביר כי יום שלישי הוא היום בו Microsoft נמצא במצב סכנתה מפני רוב התקיפות וכך ניצל את רוב המשאבים 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 תהליך הכתת 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 להרכיב שאלות פשוטות יחסית.

הקוד פועל על התוכנה באופן מקומי ישירות על מחשב האישי, 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, לבדוק מקומית מבטיחה עצמאוות מרשות תקשורת ומפחיתה סיכון.

הנתונים שהורדנו אינם מכילים את עמודות ה - ID, היא נוספת לשם מפתח ייחודי של כל תקיפה. באמצעות SQL – רצינו שאילנות מתקדמות ייחסית, 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 – מחשבי Mac לא צריכים הפעלה מחדש לאחר עדכון לuemot 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 על רמת האבטחה ותחזוקת המערכות השונות.

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

## למה SQL?

SQL ישן שאילנות שמאפשרות מייקוד 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 ונתוחים סטטיסטיים בצורה קלה ומהירה. פעולות אלו מאפשרות ליזמות מגמות, חריגות 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 bar displays "Local instance 3306 - Warning - not supported". The main window has tabs for "Administration" and "Schemas". Under "Schemas", there is a tree view with "project\_database" expanded, showing "Tables", "Views", "Stored Procedures", and "Functions". The "Tables" node is selected. The "Tables" list shows "Microsoft\_Attack". Below the tree, the "Object Info" tab is active, showing "No object selected". The "Session" tab is also visible. In the center, a "Query 1" tab is open with the following SQL code:

```

SELECT ma.ID, ma.Affected_Component, ma.Reboot, ma.SeverityPOINT1, 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" shows 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

The bottom status bar shows "Microsoft\_Attack 141".



## 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 המקורי, 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

output  
Model Prediction: ['Important']

Flag

Clear Submit



כדי לפרוס את המודול וליחסם באופן קל ונגיש בראשת, יצרנו ממשק האינטראקטיבי של Gradio והעלונו אותו ל- **Hugging Face Space**.  
פלטפורמה זו מאפשרת להפיץ את המודול לכל משתמש, ללא צורך בהרצאות מקומיות, ומציעה נוחות רבה בשימוש, ביצוע עדכנים ותחזקה. פרישה ב-Hugging Face מיעלת את השימוש וmpshetat את ההנגשה למשתמשי קצה או גורמים עסקיים.  
פלטפורמה זו מאפשרת למפתחים לפרוס ולשתחוו יישומים אינטראקטיביים מבוססי מידע מכונה.  
היא מספקת סביבה לייצור ממשקים אינטראקטיביים מביי לדאגה לתשתיית או להרצאות מקומיות.  
ניתן ליצור ממשק אינטראקטיבי באמצעות Gradio העלאת המודול לפלטפורמה מאפשרת לשתוף את המודול שלהם, זה מאפשר שיתוף פעולה, קבלת משוב, ופרישה מהירה של המודול לשימושים.

**למה Hugging Face Spaces ?**

Hugging Face Spaces מאפשרת לפרוס יישומים במהירות ובקלות, ללא צורך בתשתיות מורכבות או בהרצאות מקומיות. הפלטפורמה תומכת בשיתוף פעולה עם קהילת מפתחים רחבת. היא מאפשרת קבלת משוב ושיפור מתמיד של המודלים, וכן פרישה מהירה של גרסאות חדשות. היא מציעה גמישות ונטיגות למשתמשים וגורמים עסקיים, תוך TMICHA במנוף Hugging Face, מה שמקל על פיתוח ושימוש יעיל במודלים וניתוח נתונים. במנוף Hugging Face, ניתן מותmicah רחבה של קהילה גדולה ותיעוד נרחב, המאפשרים פתרון בעיות ולמידה משותפת. הפלטפורמה מאפשרת אינטגרציה פשוטה עם כלים ומרכיבות נוספות, כך שניתן לשלב את המודלים במערכות קיימות וליציר זרימות עבורה מורכבות. כל זאת נעשו במסגרת חיינית, המאפשרת למפתחים לפרוס מודלים ללא עלות, תוך זמן פרישה מהיר שמאפשר זמינות מהירה של גרסאות חדשות.

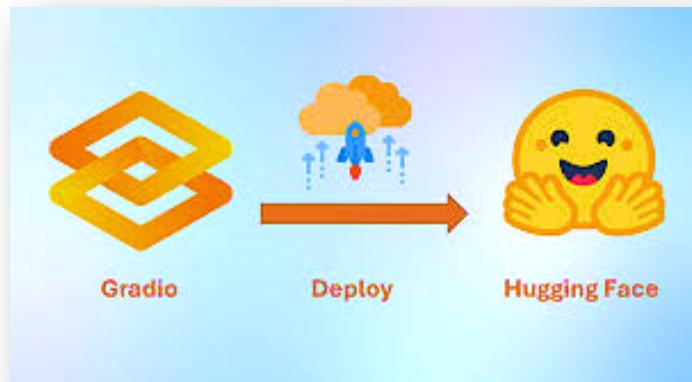
שני היתרונות המרכזיים של הפלטפורמה זו –

- חייניות :** הפלטפורמה חיינית לשימוש, מה שמאפשר למפתחים לפרוס את המודלים שלהם ללא עלות .
- זמן פרישה מהיר :** ניתן להעלות מודול ולהפוך אותו לזמן תוך זמן קצר, מה שמאפשר פרישה מהירה של גרסאות חדשות.

[Hugging Face Link](#)



Hugging Face





## 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 בפתרונות מתקומות מקצועית, כפי שפורט בפרק 1, הינס חלק בלתי נפרד מטהlixir זה, שכן הם מאפשרים שקייפות, שיתוף פעולה והמשכיות.

### מבוא לניטור ותחזוקה: הקשר לנתוני 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 הפוגעת (Affected Component). בנוסף, הנתונים כוללים אינדיקציה 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 חשיבות גבוהה 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, המוגבהה במנגנון ניטור ותחזוקה, מסייעת במניעת נזקים עתידיים, לרבות אובדן נתונים, פגעה במוניטין והשלכות כספיות, הנובעים מפגיעות 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 גודלים, ניתוח ויישום 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, ובמבטיה עמידה בתקני אבטחה מיידע מחמירים – תוצר לוואי הכרחי של תהליכי תחזוקה מוקפם.

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



## 1.2 אילו גורמים / השפעות צריכים להיות במעקב ?

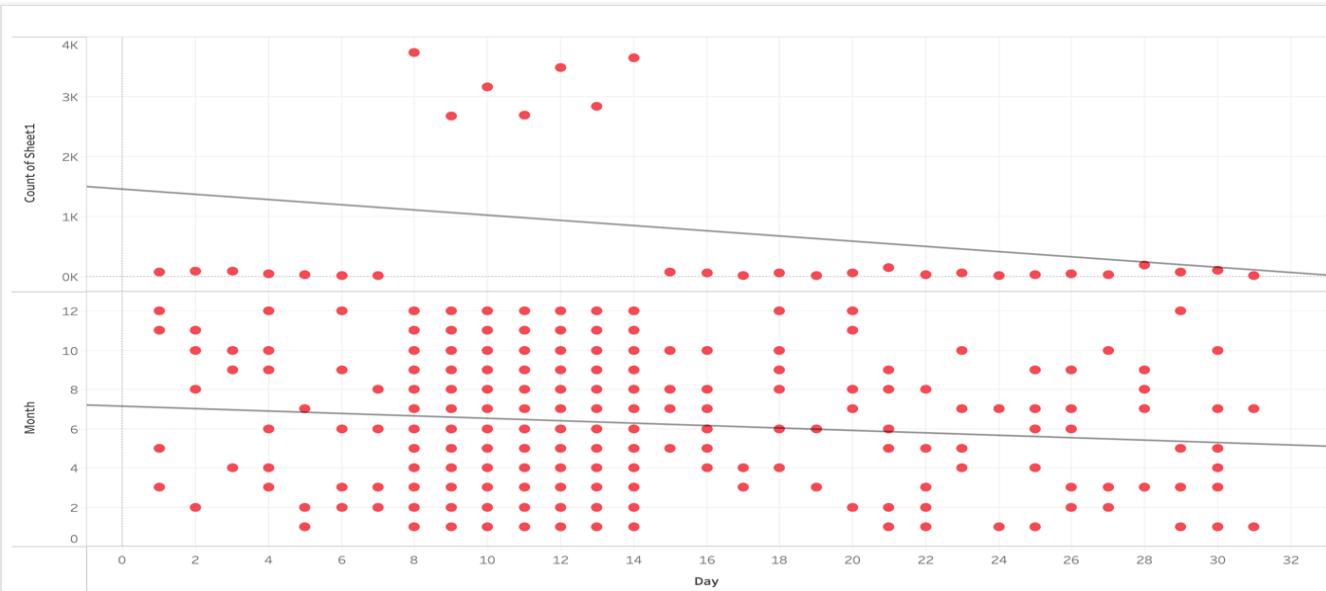
בדאטה שלנו יש הרבה מאוד לוגים שנרצה להיות במעקב אחריהם, כגון : Severity.1, Severity ו-Severity.1, Impact.1, Impact ועוד ... נזכיר את ניתוח מאפייני הנזונים שודיעו לנו בדוחות הקודמים לשם סקירה וסימון התוכנות עליהם נבצע את המעקב -

Feature Name	Definition	Description
Date Posted	The date when the bulletin was published.	Indicates when the security update or bulletin was officially released.
Bulletin Id	The unique identifier for the security bulletin.	Helps in referencing and categorizing security updates.
Bulletin KB	Knowledge Base (KB) number associated with the bulletin.	Links to detailed technical documentation about the 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 bulletins 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.

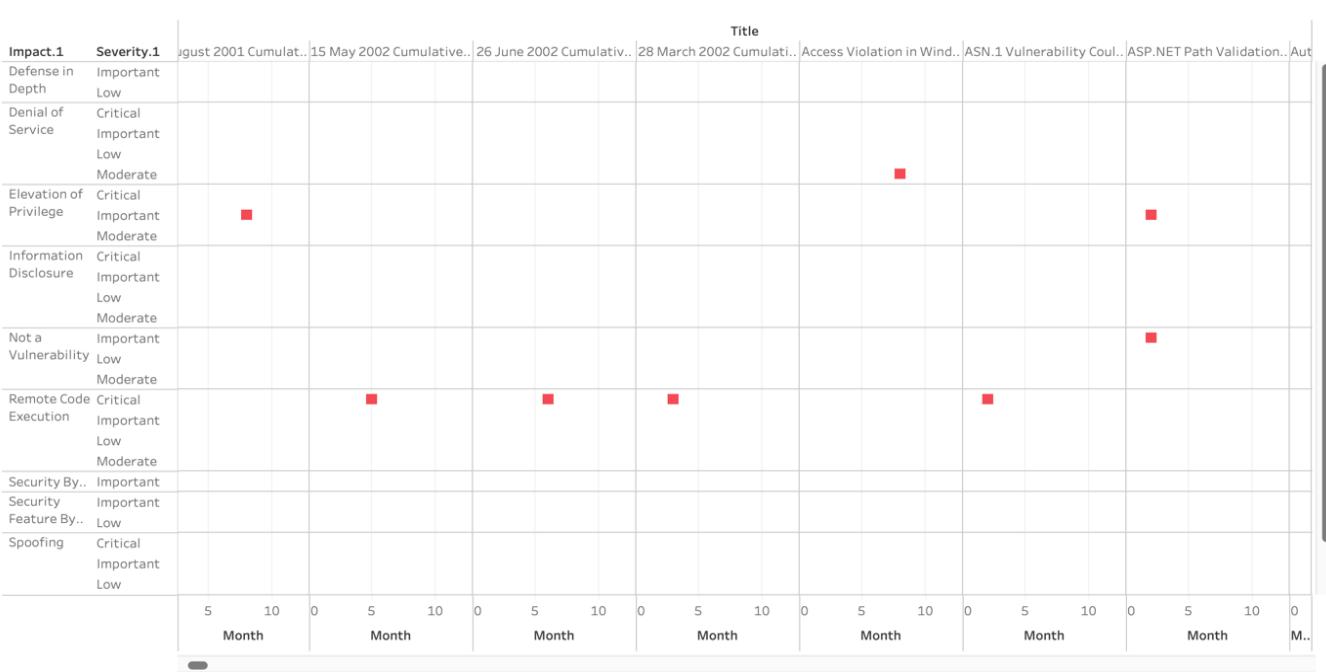
שם תכונה	הגדרה	תפקיד
תאריך פרסום	התאריך שבו פורסם לעילן.	מצינן מתי דעון האבטחה ואנו שוררו באופן رسمي.
זהה עלן	הזהה הייחודי של עילן האבטחה.	עד/or בהפנייה או ייוג עדכני אבטחה.
KB עלן	מספר מאגר ייוז (KB) המשיר לעילן.	קיים כדי ליתוד טיב פוטוטלי לעילן.
חומרה	רמת הרגישות של העדכן.	מגדיר את החשיבות של יישום העדכן, כגון קריטי, חשוב וכו'.
פעעה	סוג פגיעה שבבב העדכן פועל.	מצינן אם הפגיעה מספיעת לבעון קוד מרוחק, מניעת שירות וכו'.
טוקחת	הכוורת על עילן אבטחה או עדכן.	מספק תיאור כיצד של העדכן או מאריך.
מוצר מושפע	המוצר שמוספע מהפגיעה.	מפורט את מערכות הפעולה, היישומים או השירותים הדורשים עדכן.
ריב KB	מספר מאגר הדע (ID) (בנוסף להריב המושפע).	מצינן את התעדות חמי עירוב והריב המושפע.
ריב מושפע	הריב הספציפי המשפע מהפגיעה.	פירוט החלק של המוצר או השירות הפוך.
1.הפעעה.	תיאור שפניה מסוימת בעור בפגיעה.	בבבב דע יירא את השפנית הפעעה, בביטחון הצורה.
1.חומרה.	רמת חומרה מסוימת בעור העדכן.	סביר סואן חומרה נזק אם לאלו.
מחולף	הילן או העדכן שאחדת מהליף.	מצינן דעוכם שציאו שימוש או שאם ישם עוד.
לאתחל	האם נדרש מחדש לאחר החלת העדכן.	מצינן אם המערכת צריכה להפעיל מחדש כדי להשלים את התיקנת העדכן.
CVEs	מחוי פגיעות וחיפוי נזקאות.	מפורט מחויים סטנדרטיים עבור קבוצות טרוף, המטולות על ידי העדכן.

כפי שניתן לראות, יש לנו הרבה תוכנות קריטיות שהיינו רוצחים לבצע עליהם ואחר וכל תוכנה היא רלוונטית וכיולה להוועיל לנו בתובנות ומיציאת קשרים בהמשך לצורך חיזוי התקפות עתידיות. לצורך העניין אם יש לנו תוכנה מסווג כAffected Component או כAffected Product ניתן רוצחים לדעת ממה רמת הפגיעה שחווו או איזה ריב או מוצר/שירותות נפגע שכן אם נתקבב וננטור לוגים אלה נוכל להגיע למסקנה שאכן יש חולשה באוטו שירות או ריב. נוכל ללמד את המודל מתי, כמה ואיפה ע"פ מעקב וניטורם אילו מהי תקיפה וסיכון ממשי ומהו רישום לוג תקין במערכת.

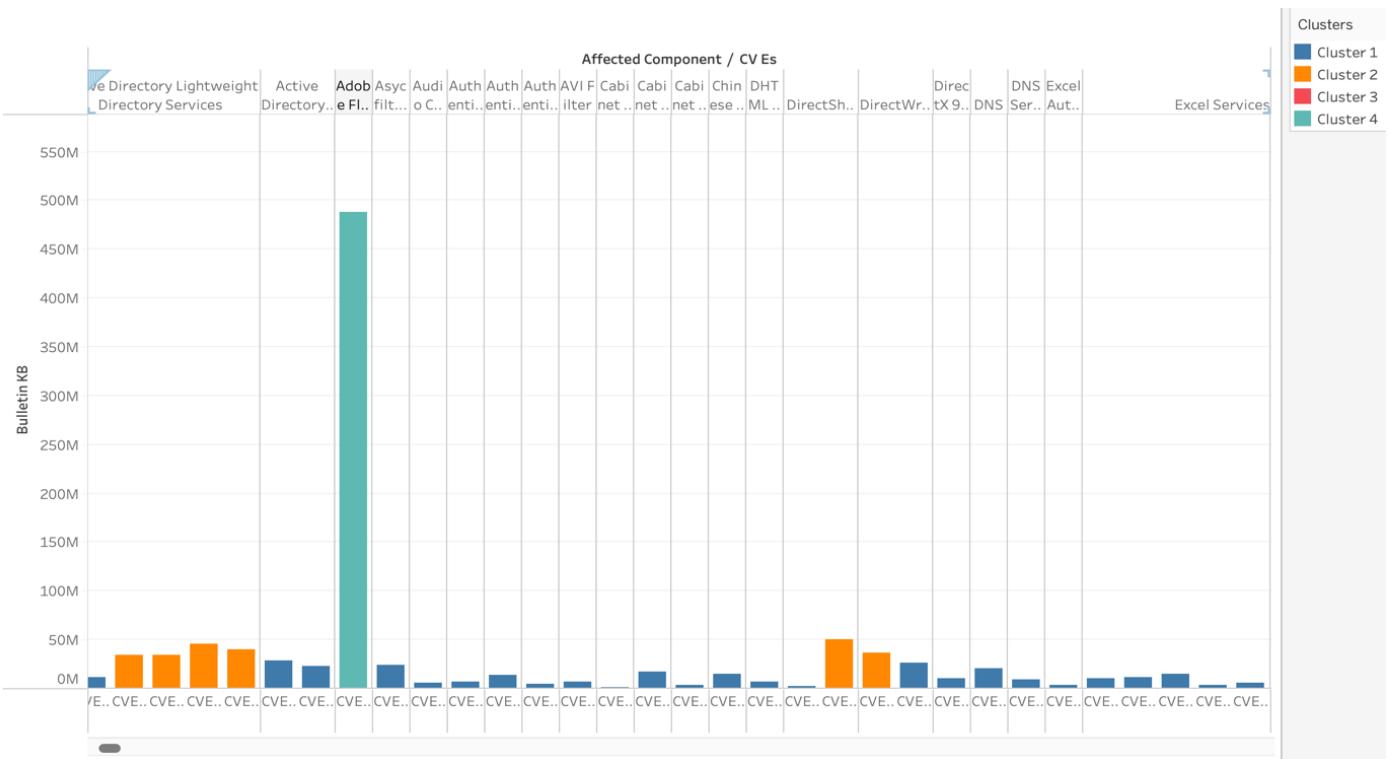
כלומר נרצה לחבר לאלגוריתם שלנו מערכת רישום (Management) מותך אותה החברה שתהיה מעוניינת בכך, ובכך ללמד את המודל בצורה richtig את הרישומים השונים שמנצאים במערכת. נראה כמה גրפים על הדאטה שלנו מתוך Tableau אשר מראים כיצד היינו מנתחים, וכייזה היו שמותם לב לאותם הלוגים הרשומים במערכת החברה.



- ניתן לראות שימושים 8 עד 14 הותקפו/ביצעו עדכנים לאורך כל החודשים. בנוסף ניתן לראות שאלות הימים לאורך החודשים שהו הכי הרבה רישומי לוג חיריגים כבן 2600 ל 3700 ( בניהם התקפות ועדכנים ).



- בגרף זה ניתן לראות את כוורות הלוג מסודרות ע"פ חודשים לצד השפעות שבתוכם יש סיווג לרמת הקriticיות של אותה ההשפעה מנמוכה לקriticית. כמו כן ע"פ גרף זה ניתן לדעת וללמוד את המודל מהי בעיה קriticית ומהי בעיה נמוכה ולפי זה נוכל ללמד אותו להזות עדכנים או מטרות שנרצה למש用工 ובקצ' למנוע התקפות עתידיות – בכך שנמנע חולשות. לצורך העניין בגרף זה ניתן לראות התקפה מסווג Elevation of Privilege (סוג התקיפה שבה התוקף מקבל הרשותות גביהות יותר ממה שモותר לו) המסוגת חשובה. בנוסף יש עוד המונח התקפות שנוכל למצוא אשר רשומות בגרף זה כמו הידועה Remote Code Execution ו-DDOS.



- בגרף זה ניתן לראות שירות שנפגע באופן קשה מאוד, המוחסן לו ככמעט חצי מיליון מיליאון מיליאונים שנפגעו מאותו שירות זה, השירות הוא Adobe Flash Player, אשר היה תוסף לדפים השונים והיה יעד אסטרטגי ל악רים 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 וдиוק 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 וניטור 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 מכלל 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.

מדידה אופטימלית	חסרון	יתרון	
ニקיי נתונים ומדדים של חוסר איזון.	לא מבחין בין סוג הטיעויות	טוב לנתחים עם מחלקות מאוזנות	Accuracy
Recall עם איזון ובפרמטרים ובצורה נכונה של המודל	חוסר איזון בניבוי אופטימי של המודל	חשוב כאשר שגיאת המודל גבוהה	Precision
Precision עם שילוב F, שימוש בנתונים מגוונים.	עלול להוביל לעליה בשגיאות הניבוי	חשוב למניעת false-negatives	Recall
שילוב מדדים נומפיים, ומניעת הטיה.	אין פירוט מלא על הטיעויות.	ממוצע הרמוני מאוזן בין Precision ו-Recall	F1 Score



בדי לנטר את התוצאות של המודלים נשתמש בשיטות שונות:

מידה אופטימלית	חסרונו	יתרונו	
השואת ביצועים על נתונים חדשים ומידה תקופתית.	דורש מעקב רציף	זיהוי ירידת מוקדמת ביצועים והתקאת המודל בזמן	מעקב אחר מגמות ביצועים לאורך זמן
IRECT Dashboards יצרת מעודכנים בזמן אמיתי וסקירותם קבועה	יכול להסתמך על פרשנות אישית	מצגת מידע ברור ואינטואיטיבי על ביצוע המודל Dashboard	ויזואלייזציה של תוצאות
שימוש בכלים סטטיסטיים ליזיהוי דיפרנציאציה ביןTONIM ומטען התראה אוטומטית	זיהוי מורכב ודורש משאבים	מניעה ירידת ביצועים בעקבות שינוי	NEYTOR SHINNOIM בתנאים
ניסוי מבוקר וברנית ביצועים סטטיסטיים	דורש משאבים זומן , לא תמיד ניתן לביצוע	ברירה מותאמת בין גרסאות	NEYSOIIM MBOOKRIM
איסוף משוב באופן , שיטתי וקבוע , להיות סובייקטיבי	לא מייצג את כלל המשמשים , יכול איוכות המודל	משפר התאמת לצרכי המשמש ומעלה את איוכות המודל	AISSOF VMSHOB MMASHMASHIM
הגדרת סף רגישות מתאים והתקאות מערכת ההתראות לאורך זמן	סיכון להתראות שגויות	מאפשר תגובה מהירה לבעיות ומונע נזקים	HTEROT

### 3.2 כיצד נקבע מתי פג התקוף של כל דגם ?

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

**undercut ביצועים לאורך זמן** - נבדוק את ביצוע המודל על **נתונים חדשים** לאורך זמן.

אם המודדים יורדים מתחת למספר שנקבע, אז המודל כבר פג וצריך לעדכן אותו או להחליפו.

**זיהוי שינויים בתנאים** - אם התפלגות התכונות שהמודל מקבל משתנה, ביצועיו של המודל יפחתו.

שינויים אלו יכולים להתרחש בעקבות, טrndims, 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.

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





## קישורים

[GitHub](#)

[Dashboard 1](#)

[Dashboard 2](#)

[Hugging Face - app](#)