

תאריך 12.09.2025

לכבוד
יחידת הפרויקטים מה"ט

הצעה לפרויקט גמר

יש להדפיס את כל הנתונים הנדרשים

א. פרטי הסטודנטים

שם הסטודנט	ת.ז. 9. ספרות	כתובת	טלפון נייד	תאריך סיום הלימודים
סאמר ג'ראיסי	315183731		0526682854	

שם המכללה: **המכללה הטכנולוגית נוף הגליל** סמל המכללה: **72209**

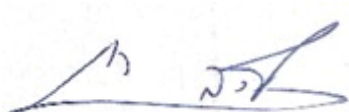
מסלול ההכשרה: **הנדסאים**

מגמת לימוד: **תוכנה בהתמחות FS**
מקום ביצוע הפרויקט: **המכללה הטכנולוגית נוף הגליל**

ב. פרטי המנחה האישי

שם המנחה *	כתובת	טלפון נייד	תואר	מקום עבודה/תפקיד
להב רון	יקינטון 23 חיפה	0523203282	Bsc/MBA	מכללת נוף הגליל

* עבור מנחה אישי חדש יש לצרף קורות חיים, ניסיון מקצועי ותעודות השכלה לאישור מה"ט.



חתימת הגורם המקצועי
מטעם מה"ט

חתימת המנחה האישי

חתימת הסטודנט

1. שם הפרויקט:

WireTracer מערכת למעקב אחרי Packets וניטור משאבי חומרה של המחשב.

2. רקע

2.1. תיאור ורקע כללי:

המערכת מעניקה יתרון משמעותי באבטחת מערכות, בין אם מדובר במשתמש יחיד או בקבוצת משתמשים. האבטחה מתבטאת במתן התראות על זיהוי חבילות רשת המעידות על מתקפה מקוונת נגד מכונת המשתמש, וכן בביצוע מעקב אחר אחוזי השימוש במשאבי חומרה, כגון זיכרון RAM, לצורך זיהוי והתראה על נוכחות של וירוס מקומי במערכת.

2.2. מטרות המערכת

בהתבסס על יכולות האבטחה המפורטות בסעיף 2.1, המערכת מציעה מנגנוני ניטור והתראה מתקדמים לזיהוי ודיווח על פעילות חריגה. באמצעות ניתוח חבילות רשת ומעקב אחר ניצול משאבי חומרה, המערכת מאפשרת איתור בזמן אמת של איומים פוטנציאליים, כגון מתקפות מקוונות או וירוסים מקומיים. התראות המערכת נועדו להבטיח למשתמשים תגובה מהירה וממוקדת, המותאמת לשמירה על תקינות המערכת ולמזעור סיכונים אפשריים.

3. סקירת מצב קיים בשוק, אילו בעיות קיימות

ישנו אוסף של טכנולוגיות אשר קיימות עם אותה פונקציונליות בשוק שלושה מהם הם הנ"ל
3.1 [WireShark](#) האפליקציה מכילה תכונות כמו תכונת צפייה בפקטות אבל אין לה את היכולת להתריע על סכנה פוטנציאלית למחשב המשתמש דרך מתקפות אנטרנטיות כמו DDOS ו-PHISHING.

3.2 [TASK MANAGER](#) במנהל המשימות של מייקרוסופט אנו יכולים לזהות את רמת השימוש במשאבי מחשב כמו RAM CPU ודיסק קשיח מה שבעייתי במנהל המשימות זה שהוא לא מאחד זיהוי דפוסים אנטרנטים יחד עם תכונתו הידועות, לכן הפרויקט שלי שואף לאחד את הפונקציונליות של מנהל המשימות יחד עם זו של WIRESHARK בתוך ממשק אחד.

3.3 [Zeek](#) היא תוכנה לניתוח תעבורת רשת, בדומה ל-Snort ו-Wireshark-המתמקדת בניטור פסיבי ותיעוד יומנים לניתוח מאוחר, כולל ניתוח HTTP, זיהוי ומעקב SSL. עם זאת DNS, היא אינה מתאימה לניטור משאבי חומרה או זיהוי איומים מקומיים ודורשת ידע טכני מתקדם. לעומת זאת, התוכנה שלנו מציעה ממשק ידידותי, התראות מיידיות, וניתוח מותאם אישית המגן מפני איומים חיצוניים ופנימיים, תוך אספקת שכבת אבטחה הוליסטית ואפקטיבית יותר.

4. מה הפרויקט אמור לחדש או לשפר

הפרויקט מיועד לספק ממשק משתמש אינטואיטיבי, המאפשר לכל משתמש, ללא קשר לרמת הידע הטכני שלו, להבין ולעבד את התראות המערכת בקלות ובהירות. הממשק עוצב בקפידה כדי להנגיש מידע קריטי בצורה ידידותית, תוך שמירה על רמה גבוהה של דיוק ואמינות. התראות המערכת יספקו מידע מפורט וזמין על איומים אפשריים, כגון וירוסים, מתקפות אינטרנטיות, או פעולות זדוניות אחרות, במטרה להעניק למשתמשים כלים אפקטיביים לזיהוי מוקדם ולתגובה מהירה. בנוסף, המערכת משלבת פתרונות חזותיים ותיאוריים המסייעים למשתמש להבין את מצב האבטחה של המערכת שלו, ומבטיחה חוויית שימוש פשוטה אך מתקדמת, שתומכת במניעת סיכונים ושיפור אבטחת המידע באופן מתמיד.

5. דרישות מערכת ופונקציונאליות

5.1. דרישות מערכת פיתוח המערכת ידרוש שימוש ב-VISUAL STUDIO בנוסף ל-API של VIRUS TOTAL וגם ניתוח פקטות המרמיזות על מתקפות אנטרנטיות על המשתמש

5.2. דרישות פונקציונאליות

מספר מזהה	דרישה ותיאור	FR	NFR
1	רישום וכניסה למערכת ובטיחות צד משתמש		
1.1	המערכת תאפשר רישום ראשוני עם אימות כתובת מייל	V	
1.2	למערכת תהיה אפשרות לאיפוס סיסמה דרך כתובת המייל של המשתמש	V	
1.3	נתונים רגישים של משתמש, כגון סיסמה, יעברו הצפנה באמצעות אלגוריתם Hashing מתקדם מסוג BCrypt	V	
1.4	אימות בקשות HTTP של המשתמש יתבצע באמצעות JWT (JSON Web Token), אשר נשלח למשתמש בעת התחברות למערכת	V	
2	ניטורי מערכת		
2.1	המערכת תבצע ניטור בזמן אמת של תעבורות רשת ותזהה דפוסים חריגים כמו דפוס SYC/TCP במספר גדול שמציגים סיכוי למתקפת DDOS	V	
2.2	המערכת תשלח התראה מיידית במקרה של מתקפות כמו DDOS או PHISHING	V	
2.3	המערכת תעקוב אחרי ניצול CPU, RAM ודיסק קשיח ותתריע על שימוש חריג	V	
3	התראות בזמן אמת		
3.1	המערכת תספק התראות ברורות במקרה של זיהוי דפוסים חשודים המעידים על מתקפות סייבר או איומים מקומיים, כגון וירוס המתחזה לקובץ תקין. בנוסף, המערכת תאתר שימוש יתר במשאבי החומרה ותתריע על כך בזמן אמת	V	
3.2	ההתראות יכללו מידע על סוג האיום, מקורו, והמלצות לפעולה	V	
3.3	פונקציונאליות ההתראה בזמן אמת תנוהל ע"י API של שקעים (SOCKETS) שגם יהיה חלק מתהליך ניטור דפוס אינטרנט.	V	
4	ממשק משתמש		
4.1	התצוגה תציג נתוני רשת ומשאבים בצורה גרפית וברורה. ניתוני הרשת יוצגו ע"י תיבות טקסט המכילות את סוג הפקטה, זמן הגעתה, צבע התיבה יראה את רמת סיכון פקטה (אדום, צהוב, ירוק)	V	
4.2	ניצול משאבי המחשב יוצג באמצעות תרשים מעגלי פתוח, בו יוצגו אחוזי השימוש במשאבים השונים. צבע המעגל יתאים לרמת השימוש, לדוגמה: ירוק לניצול נמוך, צהוב לניצול בינוני, ואדום לניצול גבוה.	V	
4.3	הנתונים עבור כל דפוס שנשלח מהשרת יוצגו בתוך כרטיסיה, ויכללו את הפרטים הבאים: א. סוג פקטה כגון UDP/TCP ... ב. מקור ויעד הפקטה (כתובת IP)		V

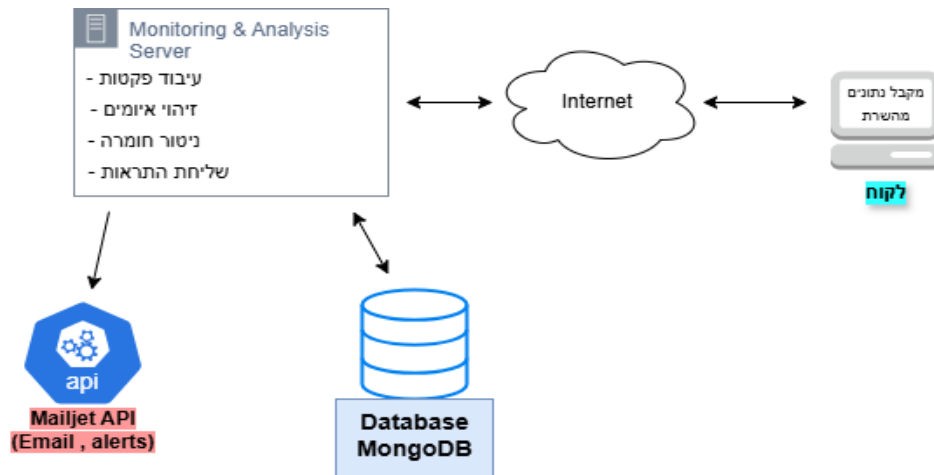
		ג. תיאור קצר על סוג הפקטה	
		דוחות וגרפים	5
	V	המערכת תייצא דוחות מפורטים הכוללים : <ul style="list-style-type: none"> פעילות רשת : תעבורת רשת לפי IP, סוג פרוטוקול (UDP/TCP), וזיהוי איומים. משאבי חומרה : ניצול CPU, RAM, ודיסק קשיח לאורך זמן. 	5.1
V		המערכת תשלח מיילים לשם התראת המשתמש על דפוסים מסוכנים במידה שהמשתמש היה רחוק מהמחשב. מיילים אלו יכללו תיאור קצר על פקטה מסוכנת ואיך בדרך כלל היא משומשת ע"י גורמים זדוניים	5.2
V		המשתמש יכול לסנן את התצוגה בממשק כך שתציג את כל סוגי הפקטות או פקטות מסוג מסוים בלבד, בהתאם להעדפתו	5.3
V		ניתן יהיה להציג גרפים על שימוש במשאבי חומרה לאורך זמן	5.4
		בינה בטחונית-Security Intelligence	6
	V	המערכת תזהה מתקפת DDoS באמצעות ניתוח וספירה של פקטות TCP/SYN	6.1
	V	המערכת מסוגלת לזהות מתקפות מסוג IP Spoofing על ידי השוואה בין כתובת ה-IP לכתובת ה-MAC של הגורם המזוהה כמחופש.	6.2
	V	המערכת מבצעת בדיקה של גודל כל פקטה על מנת להתריע בפני המשתמש על מתקפות כמו Ping of Death . פקטות חריגות הן בדרך כלל בגודל העולה על 65,535 בתים.	6.3
	V	המערכת מזהה מתקפת Smurf באמצעות בדיקת פקטות ICMP המופנות לכתובת השידור (BROADCAST ADDRESS). בכתובת ברירת המחדל מדובר ב-255, אך בתצורות רשת הכוללות Subnetting, כתובת השידור עשויה להשתנות בהתאם לטווח הכתובות של תת-הרשת.	6.4
	V	המערכת מסוגלת לזהות מתקפות מסוג Land Attack על ידי בדיקה של כתובת ה-IP המקורית והכתובת היעד. אם שתי הכתובות זהות, המערכת תתריע בפני המשתמש	6.5

6. בעיות צפויות במהלך הפיתוח ופתרונות:

תיאור הבעיה(6.1)	פתרון אפשרי(6.2)
שילוב ספריות חיצוניות (SharpPcap, PacketDotNet, BCrypt, MongoDB Driver) עלולה לגרום לשגיאות בזמן ריצה ואי-תאימות גרסאות..	קיבוע גרסאות (version pinning) בדיקות יחידה ואינטגרציה, שימוש בדוגמאות מהתיעוד הרשמי, והרצת CI מקומית לפני מיזוג.
כשלי מידע בזמן אמת בניטור חבילות רשת ונתוני חומרה תחת עומס.	שימוש ב-SignalR/WebSockets-לעדכון רציף, מדיניות retry עם cache backoff, לטווח קצר, והצגת הודעת fallback ידידותית כשאין נתונים.
עומס גבוה עקב נפח פקטות גדול (CPU/IO גבוה, קפיצות בזיכרון).	סינון בקצה (BPF filters) עיבוד באצוות (batching), טבעת זיכרון (ring buffer) עם back-pressure, אינדקסים ב-MongoDB ו-TTL-לארכיוני לוגים.
הרשאות וחסימות NIC שמונעות capture תקין בסביבות שונות(Windows 10/11).	התקנה וקונפיגורציה של WinPcap/Npcap בהרשאות מנהל, בדיקות התקנה אוטומטיות, ותיעוד דרישות הרשאה למשתמש.
סיכוני אבטחה : דליפת נתונים, אימות לקוי, שימוש לא מורשה במפתחות API, מתקפות (DDoS/Phishing).	HTTPS, אימות JWT בצד שרת, הצפנת סיסמאות עם BCrypt, ניהול סודות ב-appsettings.secrets/ENV, rate-limiting ו-input validation.

7. פתרון טכנולוגי נבחר:

7.1. טופולוגית הפתרון- פרישת המערכת



7.2. טכנולוגיות בשימוש

Visual Studio Code
MongoDB Compass
Mailjet
VirusTotalAPI

7.3. שפות הפיתוח:

צד לקוח:

HTML, CSS, JAVASCRIPT

השפות השימושיות ביותר לפיתוח אפליקציות וויב

צד שרת:

- C#

שפה עילית אשר בה ניתן לגשת לחומרה על מנת לקבל נתונים. הייתי צריכים להשתמש בה על מנת לשלוח מידע על דפוס רשת ואחוזי שימוש בחומרה

בסיס נתונים:

MongoDB

מסד נתונים NoSQL עם ספריה ב-C# המספקת פיצ'רים לניהול נתונים

7.4. תיאור הארכיטקטורה הנבחרת- הסבר בכמה מילים מדוע

בחרתי בארכיטקטורת שרת-לקוח כדי לספק מידע ללקוח שלי דרך שימוש בשרת לוקאלי עם הפיצ'רים ה-Low level של C# וזאת משום ש-JAVASCRIPT אינה יכולה לגשת לחומרה כמו C# במקביל JS מנהלת את הצגת האנפורמציה למשתמש בצורה ברורה

7.5. חלוקה לתכניות ומודולים

מחלקת MetricsFetcher: מחלקה אחראית על שליפת אחוזי שימוש בחומרה המחלקה מכילה מתודה ראשית בשם GetMetrics מתודה זו מחזירה אחוזי שימוש במשאבים בצורת רשימה לשם שליחתם למשתמש.

מחלקת PerformanceHub: מחלקה המקבלת אחוזים מ-MetricsFetcher לשם שליחתם למשתמש בנוסף המחלקה מעדכנת ערכים קריטיים אחרי כל מדידת אחוז שימוש כמו ממוצע שימוש וסטיית תקן של אחוזי שימוש בחלק חומרה מסויים.

מחלקת CaptureService: מחלקה זו שולפת פקטות מכרטיס הרשת ומעבירה אותם למנטר, המחלקה שומרת שדה של תור אשר בו יש מידע על פקטות שנשלפו. אותו תור שומר מידע על הפקטות אחרי ניטורן ושולח אותם למחלקה ששולחת אותם ללקוח לפני מחיקתם

מחלקת PacketHub: מחלקה אשר מקבלת את הפקטות אחרי ניטורן ושולחת אותם ללקוח, המחלקה מכילה פונקציה בשם GetPackets שצד הלקוח קורא לה באופן אוטומטי פעם אחת כל דקה.

מחלקת Analyzer: מחלקה שיש בה פונקציות לנטר פקטות 5 פונקציות לשם ניטור סוגי מתקפות שונות למשל DetectSynFlood ו DetectUdpFlood אחראיות על בדיקת מתקפות דרך פקטות TCP וudp בסדר זה. במקביל DetectPingOfDeathV4/V6 הינם לבדיקת Ping of death וכל אחת מהם בודקת סוג IP אחד לחוד

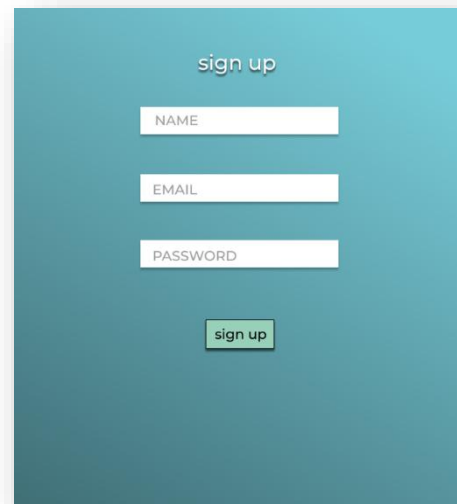
מחלקת UserController: מחלקה שמיכילה פעולות HTTP של משתמשים כמו כניסה והרשמה וגם מכילה את פיצ'ירי בדיקת קבצים וקישורים דרך API של VirusTotal המחלקה שולפת מפתחות ה-API מקובץ appsettings.json.

7.6. סביבת השרת (מקומי, וירטואלי, ענן, שירות אירוח)

לפי דרישות התוכנה הזו השרת צריך להיות מקומי בשל שליפת נתוני שימוש חומרה, ונתוני פקטות של המשתמש שלי. אם השרת לא היה מקומי אז שליפת הפקטות ונתוני החומרה תשלח את נתוני המכונה אשר עליה יושב השרת.

7.7. ממשק המשתמש/לקוח - GUI :

עמוד רישום כמשתמש



sign up

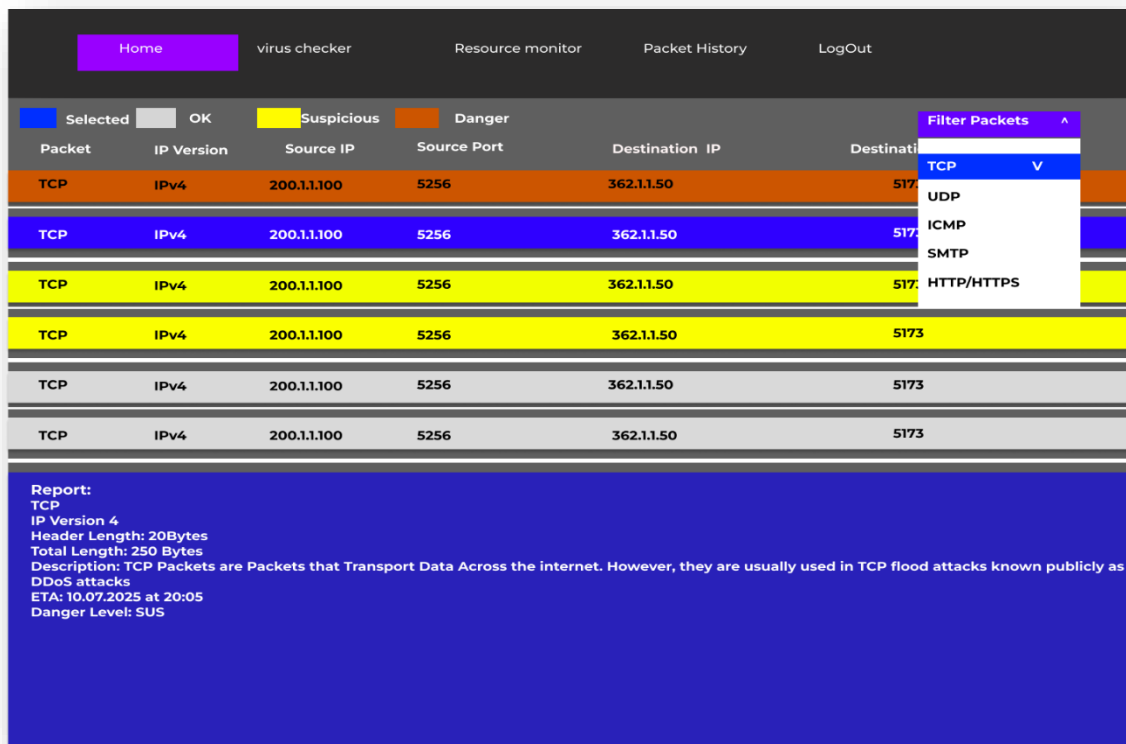
NAME

EMAIL

PASSWORD

sign up

עמוד בית (מציג פקטות)



Home virus checker Resource monitor Packet History LogOut

Selected OK Suspicious Danger

Packet	IP Version	Source IP	Source Port	Destination IP	Destination Port
TCP	IPv4	200.1.1.100	5256	362.1.1.50	5173
TCP	IPv4	200.1.1.100	5256	362.1.1.50	5173
TCP	IPv4	200.1.1.100	5256	362.1.1.50	5173
TCP	IPv4	200.1.1.100	5256	362.1.1.50	5173
TCP	IPv4	200.1.1.100	5256	362.1.1.50	5173
TCP	IPv4	200.1.1.100	5256	362.1.1.50	5173

Filter Packets

- TCP
- UDP
- ICMP
- SMTP
- HTTP/HTTPS

Report:
TCP
IP Version 4
Header Length: 20Bytes
Total Length: 250 Bytes
Description: TCP Packets are Packets that Transport Data Across the internet. However, they are usually used in TCP flood attacks known publicly as DDoS attacks
ETA: 10.07.2025 at 20:05
Danger Level: SUS

Home

virus checker

Resource monitor

Packet History

LogOut

Check Link

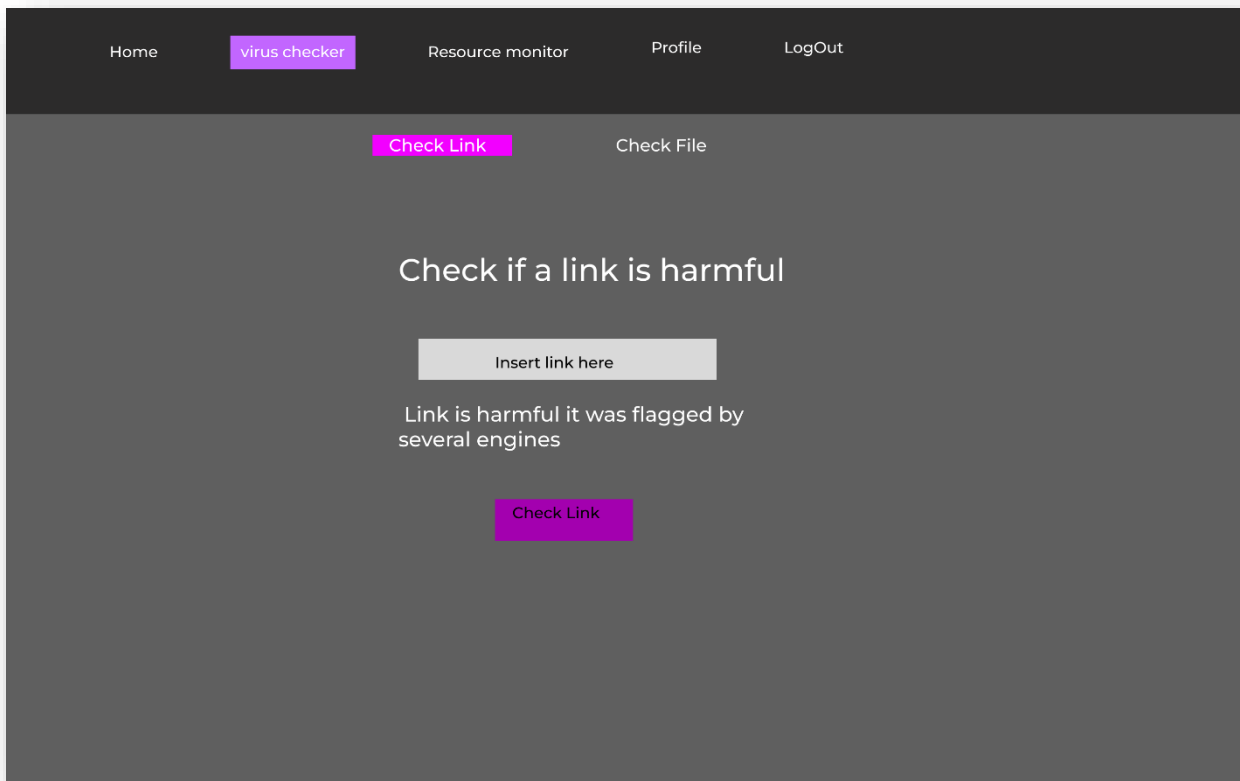
Check File

check if a file is harmful

Insert file here

This file is malicious. It was flagged
by one or more scanning engines.

Check File



[Home](#)
[virus checker](#)
[Resource monitor](#)
[Packet History](#)
[LogOut](#)

						Filter by time ^	Filter Packets ^
						1 hour ago	TCP V
TCP	IPv4	200.1.1.100	5256	362		1 Day ago V	UDP
TCP	IPv4	200.1.1.100	5256	36		7 Days ago	ICMP
						14 Days ago	SMTP
TCP	IPv4	200.1.1.100	5256	362.1.1.50			HTTP/HTTPS
TCP	IPv4	200.1.1.100	5256	362.1.1.50	5173		
TCP	IPv4	200.1.1.100	5256	362.1.1.50	5173		
TCP	IPv4	200.1.1.100	5256	362.1.1.50	5173		

Generate Report

Homevirus checkerResource monitorPacket HistoryLogOut

Timestamp:
April 18, 2025 — 14:36:42.128

Source IP & Port: 192.168.0.12:54832

Destination IP & Port: 93.184.216.34:443

MAC Addresses:
Src: 00:1A:2B:3C:4D:5E
Dst: 00:9F:12:34:56:78

Packet Type: TCP (HTTPS)

IP Version: IPv4

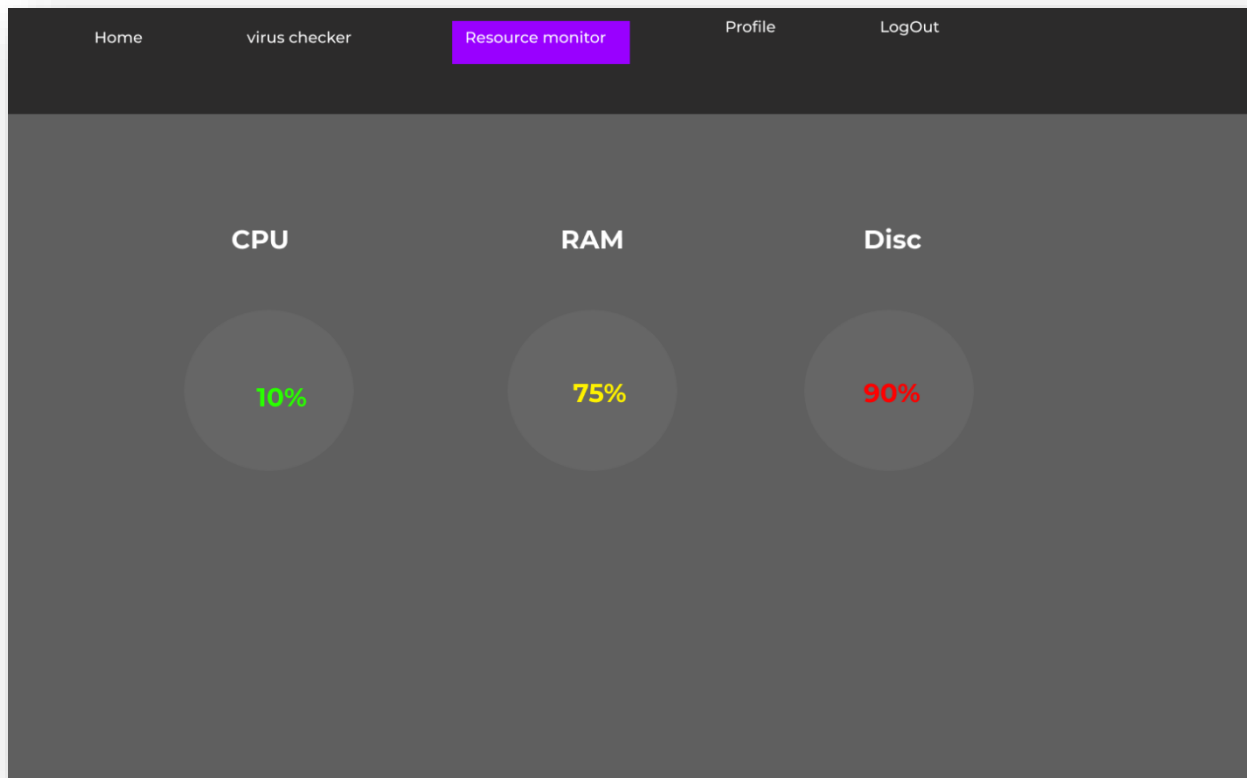
Packet Size: 1,024 bytes

TCP Flags: SYN, ACK

Direction: Outbound

Application Layer Data:
TLS Handshake Initiated
User-Agent: Mozilla/5.0 (Windows NT 10.0...)

Danger Level:
⚠️ Medium — First contact with external IP on uncommon port



7.8. ממשקים למערכות אחרות / API :

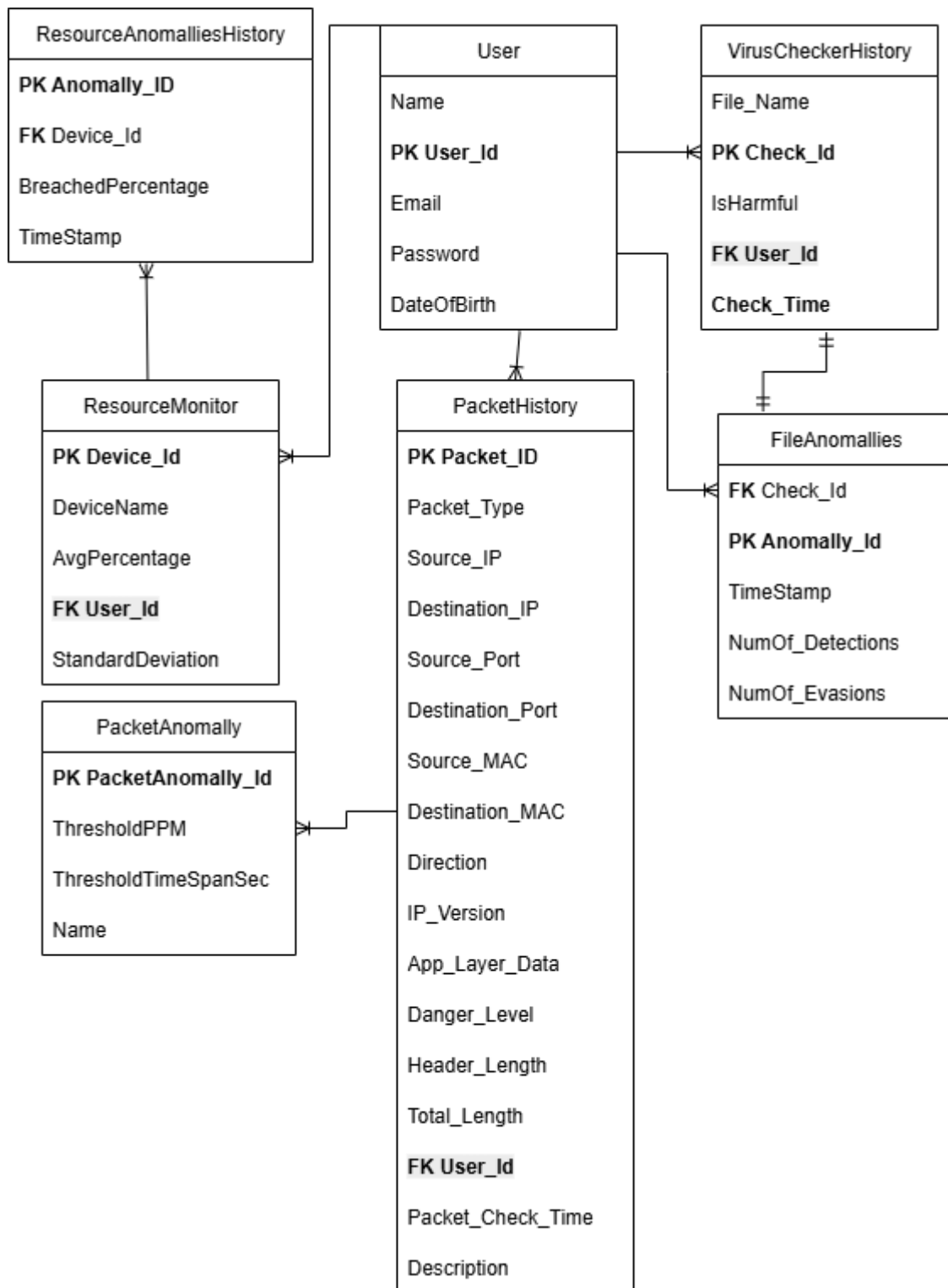
Mailjet API: לשם שליחת מיילים למשתמשים בעת שימוש יתר בחומרה, דפוסים זדוניים ו קבצים וקישורים בעייתיים ישלחו התרעות למשתמש.
Virus Total API: שנותן יכולת למשתמשים לבדוק קבצים וקישורים זדוניים ה-API מחזיר תוצאות בדיקת קובץ וקישור ותוכנה שלי משתמשת בהם לשלוח התרעה מתאימה למשתמשים בה.

7.9. שימוש בחבילות תוכנה :

PacketDotnet: ספריה שנותנת לי את הגישה למחלקות שעוזרות לי לשלוח מידע על פקטה
SharpPcap: הספריה שעוזרת לשלוח את הפקטות מכרטיס הרשת
QuestPDF: ספריה שנותנת לי את היכולת להכין תבניות טפסים שאותם אני שולח דרך המייל
BCrypt.Net: ספריה אחראית על הצפנת מידע כגון סיסמאות משתמשים. הספריה מסתמכת על אלגוריתמי Hashing לעשות זאת
MongoDB.Driver: ספריה שנותנת לי את היכולת לגשת לחלק מהפונקציונאליות של MongoDB
MongoDB.Driver.Core: החלק המשלים של MongoDB.Driver שנותנת לי גישה לעוד פונקציונאליות במסד הנתונים

8. שימוש במבני נתונים וארגון קבצים

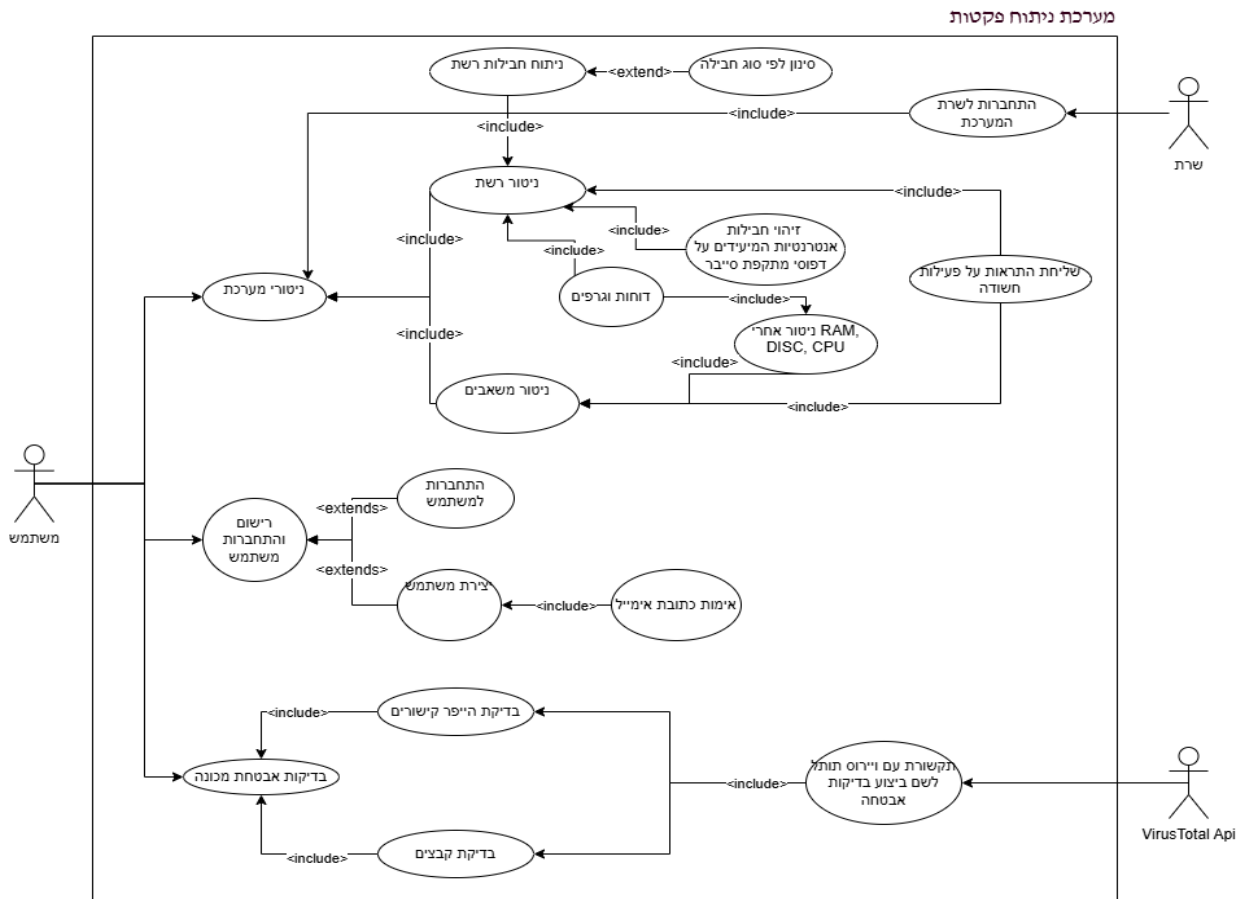
8.1. נא פרט את מבני הנתונים.



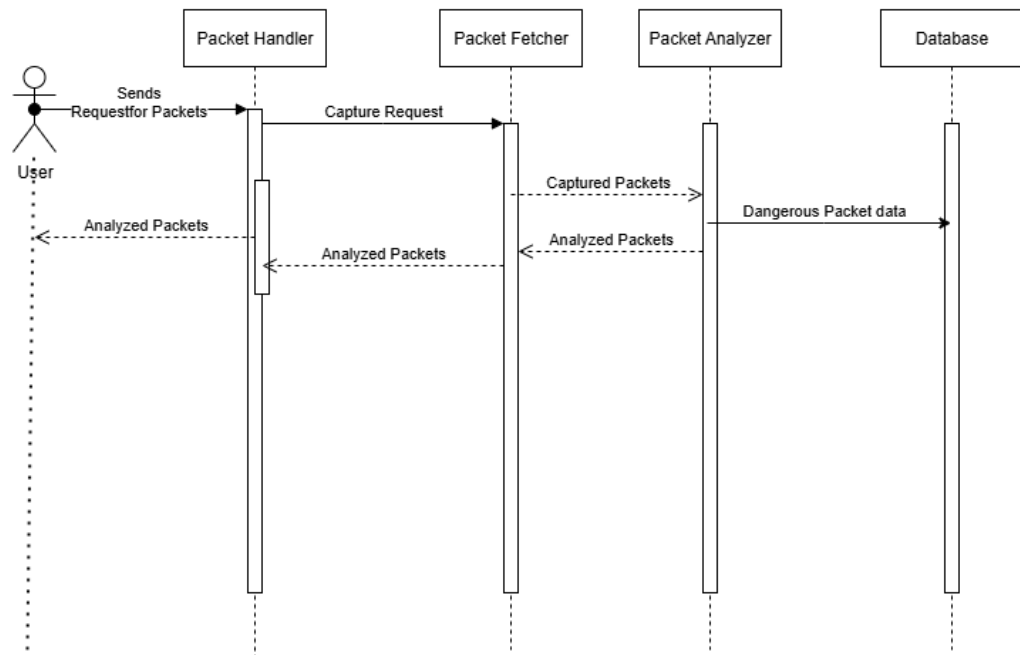
- 8.2. נא פרט את שיטת האחסון (מאגר, קבצים ובאיזה טכנולוגיה)
- 8.3. נא ציין מנגנוני התאוששות מנפילה/קריסה/תמיכה בטרנזקציות.

9. תרשימי מערכת מרכזיים

9.1 Use Case

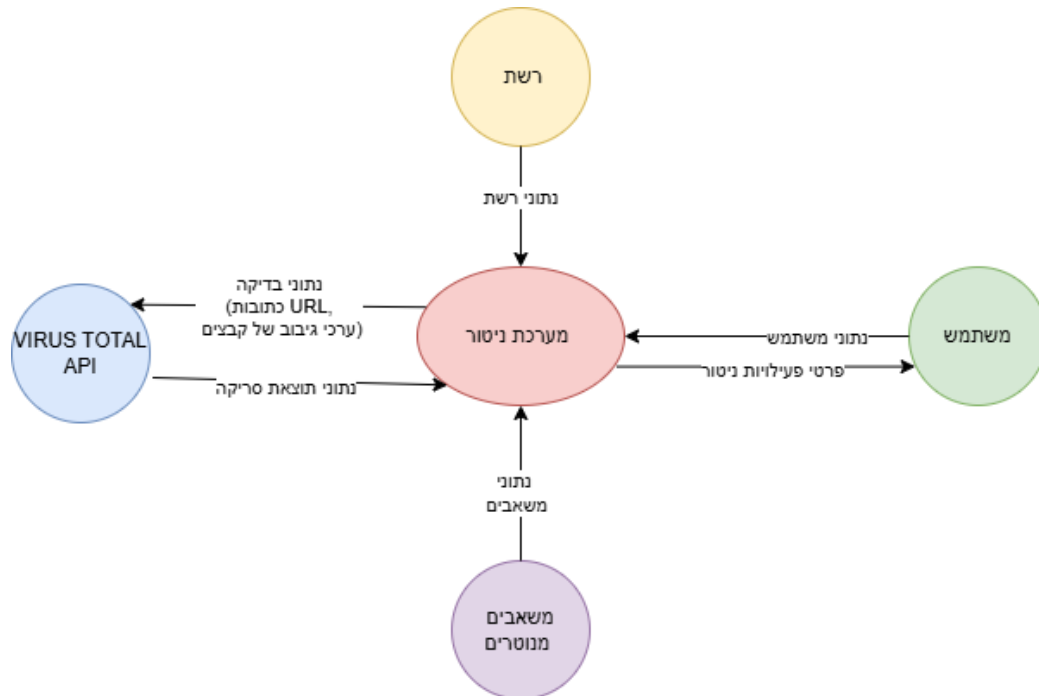


Packet Fetching Sequence

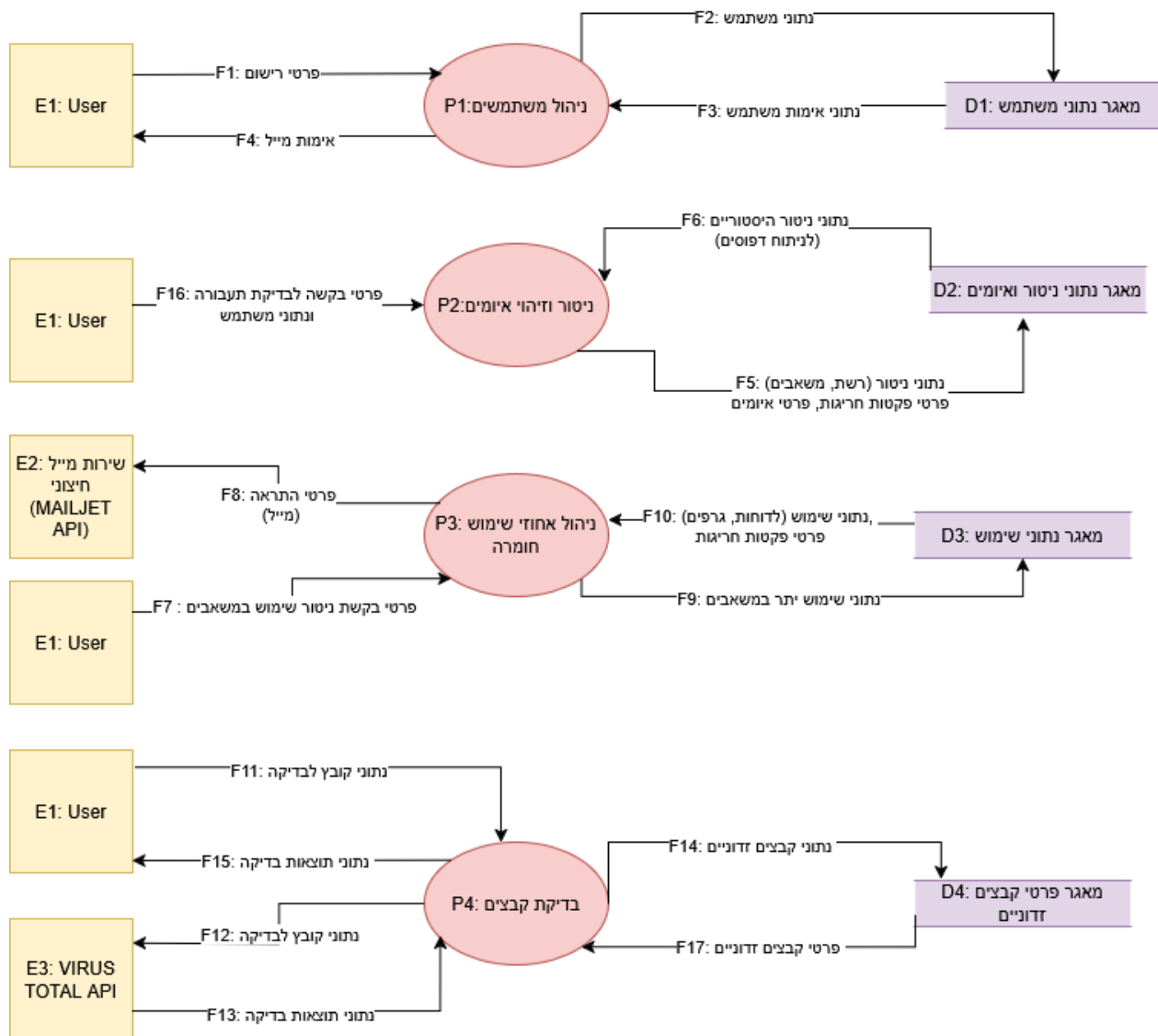


Data flow 9.1

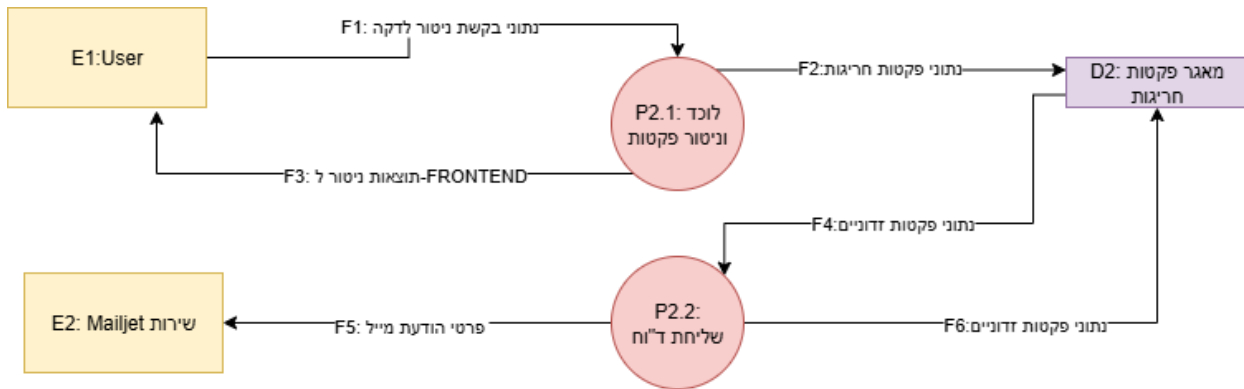
Context Diagram



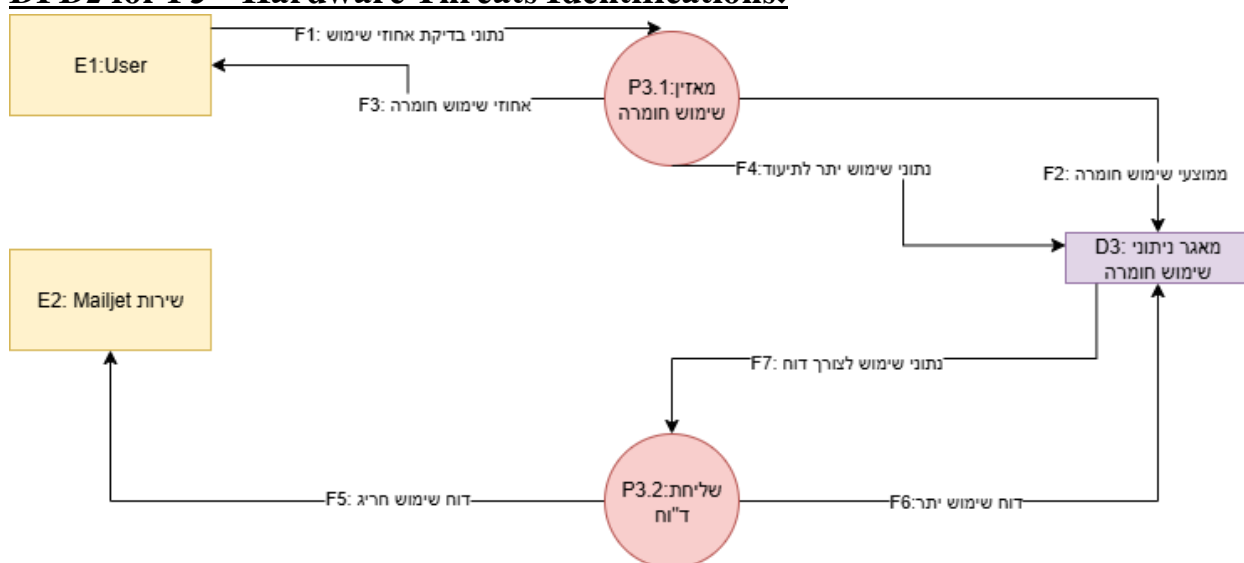
DFD0



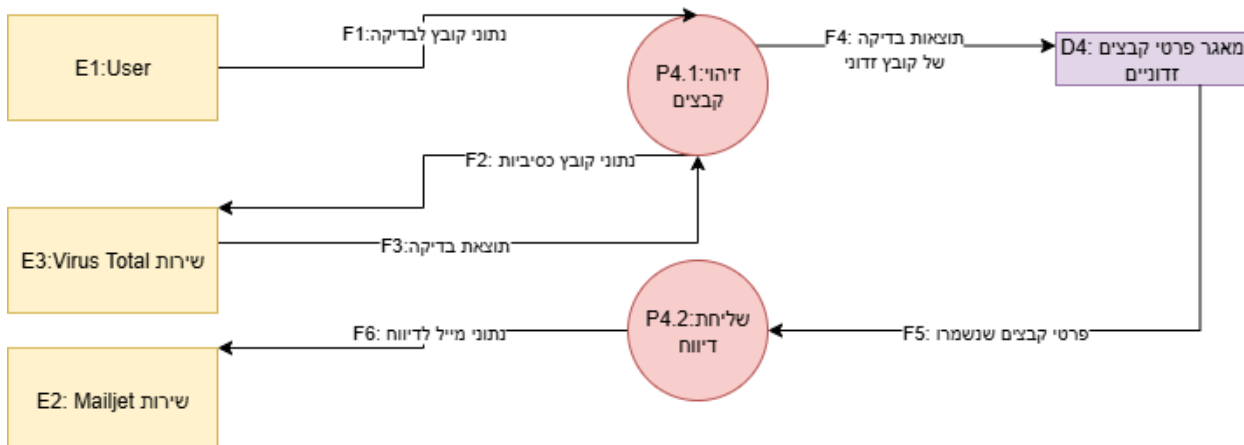
DFD1 for P2 – threat Identifications



DFD1 for P3 – Hardware Threats Identifications.



DFD 1 for P4 – Files Threats Identifications



מילונים

מילון ישויות:

קוד	שם	תיאור
E1	משתמש	המשתמש שיכול לבצע פעולות במערכת
E2	Virus total API	API הנותן את היכולת למשתמש לבדוק אם קובץ מסוים הוא זדוני או לא
E3	Mailjet API	API העוזר בשליחת דוחות לדיווח פקטות זדוניים, שימוש יתר, או קובץ זדוני

מילון תהליכים:

קוד	שם	תיאור
P1	ניהול משתמשים	תהליך המנהל פעולות הכניסה והרישום של משתמשים
P2	ניטור וזיהוי איומים	פעולה העוזרת לנטר פקטות
P2.1	לוכד וניטור פקטות	פעולה שלוכדת פקטות ושולחת אותם למנטר לפני החזרתם למשתמש
P2.2	שליחת ד"וח	פעולה ששולחת ד"וח של תוצאת ניטור פקטות למייל משתמש
P3	ניהול נתוני שימוש במשאבים	מנהל התראות לפעולת בדיקת אחוזי שימוש בחומרה.
P3.1	מאזין שימוש חומרה	מאזין וחשב אחוז השימוש בקומפוננטים של החומרה
P3.2	שליחת ד"וח	מנהל שליחת דוחות של תוצאות אחוזי שימוש בחומרה
P4	בדיקת קבצים	מנהל בדיקת קבצים שלמשתמש יש חשש שהם זדוניים
P4.1	זיהי קבצים	תהליך שמקבל קבצים ושולח אותם ל-API של Virus total לשם בדיקת רמת סכנתו של הקובץ
P4.2	שליחת ד"וח	תהליך ששולח דוחות המדווחות על סכנת קובץ אשר נבדק דרך שימוש בתהליך מס' 4.1

מילון מאגרי מידע

שדות הטבלה	שם הטבלה	שם מאגר	קוד
UserId Name Email Password DateOfBirth	User	מאגר נתוני משתמש	D1
Packet_ID Packet_Type Source_IP Destination_IP Source_Port Source_MAC Destination_MAC Direction IP_Version AppLayerData Danger_Level Header_Length Total_Length User_ID Packet_Check_Time Description	PacketHistory	מאגר פקטות חריגות	D2
Anomaly_ID Device_ID BreachedPercentage TimeStamp	ResourceAnomalyHistory	מאגר נתוני שימוש	D3
File_Name CheckID IsHarmful User_ID Check_Time	VirusCheckerHistory	מאגר פרטי קבצים זדוניים	D4

מילון זרימות מידע

שדות זרימה	יעד	מקור	שם הזרימה	קוד
*Email *Password Date of Birth Name	P1	E1	פרטי רישום	F1
*Email *Password Date of Birth Name	D1	P1	נתוני משתמש	F2
Email Password	P1	D1	נתוני אימות משתמש	F3
Email Encrypted password, Date of birth	E1	P1	אימות מייל	F4
משאבים AvgPercentage	D2	P2	נתוני רשת אוו משאבים	F5

רשת Packet_Type Source_IP Destination_IP Source_Port Destination_Port Source_MAC Destination_MAC Direction IP_Version App_Layer_Data Danger_Level Header_Length Total_Length Packet_Check_Time Description				
Packet_Type Source_IP Destination_IP Source_Port Destination_Port Source_MAC Destination_MAC Direction IP_Version App_Layer_Data Danger_Level Header_Length Total_Length Packet_Check_Time Description	P2	D2	נתוני ניטור דפוסים	F6
Email	P3	E1	פרטי בקשת ניטור שימוש במשאבים	F7
Packet_Type Source_IP Destination_IP Source_Port Destination_Port Source_MAC Destination_MAC Direction IP_Version App_Layer_Data Danger_Level Header_Length Total_Length Packet_Check_Time Description	E2	P3	פרטי התראת מייל	F8
Email	D3	P3	נתוני שימוש יתר במשאבים	F9
Packet_Type Source_IP Destination_IP	P3	D3	נתוני שימוש לדוחות וגרפים	F10

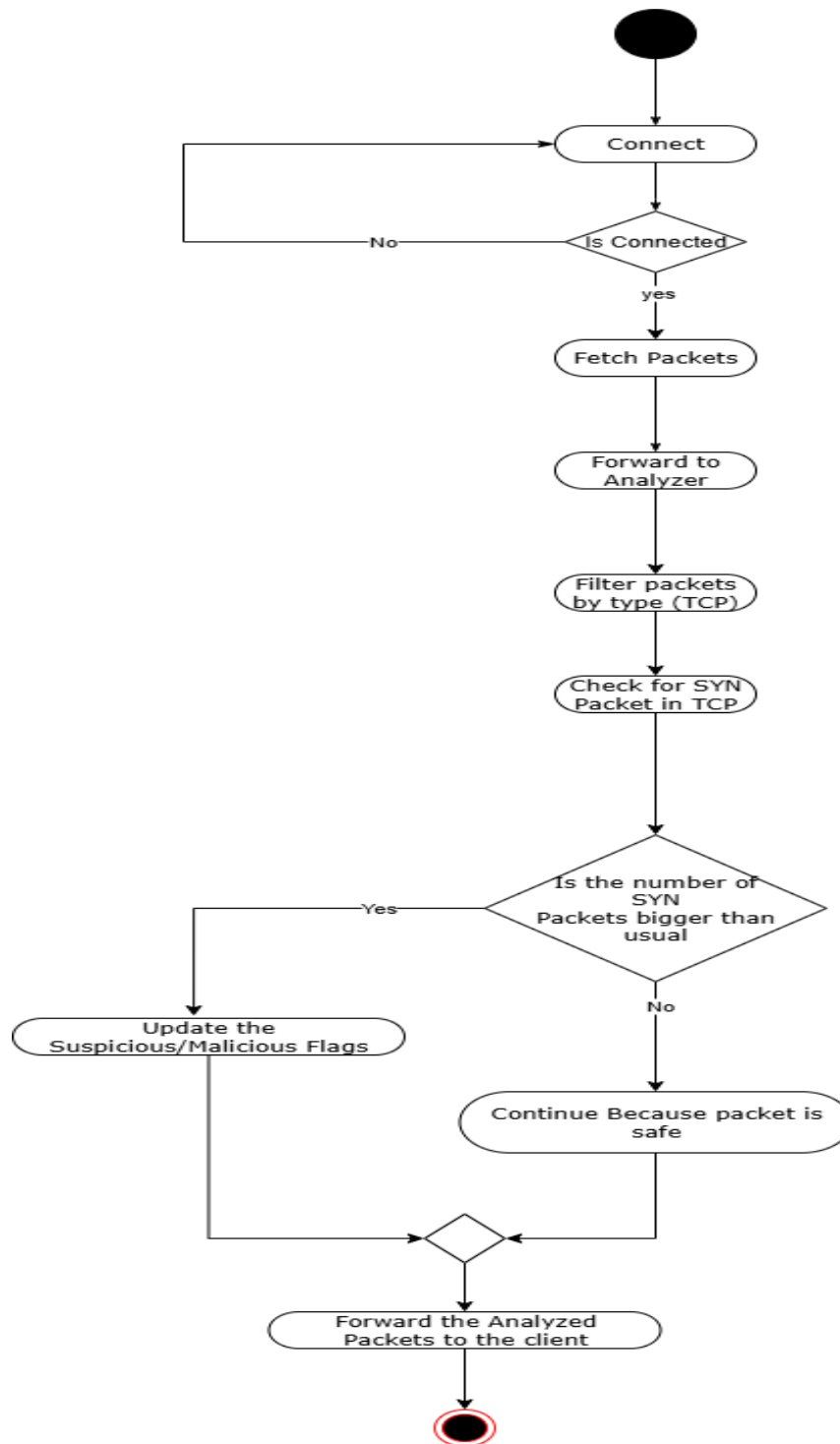
Source_Port Destination_Port Source_MAC Destination_MAC Direction IP_Version App_Layer_Data Danger_Level Header_Length Total_Length Packet_Check_Time Description				
File bytes, Email	P4	E1	נתוני קובץ לבדיקה	F11
File Bytes	E3	P4	נתוני קובץ לבדיקה	F12
Anti-Virus-Name Is malicious	P4	E3	נתוני תוצאות בדיקה	F13
Name, Date, Result, userId	D4	P4	נתוני קבצים זדוניים	F14
Name, Date, Result,	E1	P4	נתוני תוצאות בדיקה	F15
Session id	P2	E1	פרטי ברשה לבדיקות תעבורה ומשאבים	F16
Name, Date, Result	P4	D4	פרטי קבצים זדוניים	F17
נתוני זרימות ל-P2				
Session id	P2.1	E1	נתוני בקשת ניטור לדקה	F1
Source_IP Destination_IP Source_Port Destination_Port Source_MAC Destination_MAC Direction IP_Version App_Layer_Data Danger_Level Header_Length Total_Length Packet_Check_Time Description	D2	P2.1	נתוני פקטות חריגות	F2
Source_IP Destination_IP Source_Port Destination_Port Source_MAC	E1	P2.1	תוצאות ניטור ל-Frontend	F3

Destination_MAC Direction IP_Version App_Layer_Data Danger_Level Header_Length Total_Length Packet_Check_Time Description				
Source_IP Destination_IP Source_Port Destination_Port Source_MAC Destination_MAC Direction IP_Version App_Layer_Data Danger_Level Header_Length Total_Length Packet_Check_Time Description	P2.2	D2	נתוני פקטות זדוניים	F4
Email + Source_IP Destination_IP Source_Port Destination_Port Source_MAC Destination_MAC Direction IP_Version App_Layer_Data Danger_Level Header_Length Total_Length Packet_Check_Time Description	E2	P2.2	פרטי הודעת מייל	F5
-	D2	P2.2	נתוני פקטות זדוניים	F6
נתוני זרימות ל-P3				
Session id	P3.1	E1	נתוני בדיקת אחוזי שימוש	F1
AvgCpuUsage AvgRamUsage AvgDiskUsage	D3	P3.1	ממוצעי שימוש חומרה	F2
cpuUsage, ramUsage, diskUsage	E1	P3.1	אחוזי שימוש חומרה	F3
AvgUsage DeviceName Standard Deviation	D3	P3.1	נתוני שימוש יתר לתיעוד	F4

DeviceName AvgUsagePercentage UsagePercentage StandardDeviation	E2	P3.2	דוח שימוש חריג	F5
AvgUsagePercentage DeviceName StandardDeviation	D3	P3.2	דוח שימוש יתר	F6
AvgPercentage DeviceName StandardDeviation	P3.2	D3	נתוני שימוש לצורך דוח	F7
נתוני זרימות ל-P4				
File bytes, Email	P4.1	E1	נתוני קובץ לבדיקה	F1
File bytes	E3	P4.1	נתוני קובץ כסיביות	F2
MaliciousFlagNumber, OkFlagNumber	P4.1	E3	תוצאת בדיקה	F3
FileName Date of Check Num_Of_Detections, Num_Of_Evasions	D4	P4.1	תוצאות בדיקה של קובץ זדוני	F4
UserId	P4.2	D4	פרטי קבצים שנשמרו	F5
Email, FileName, Date of Check, Num_Of_Detections, Num_Of_Evasions	E2	P4.2	נתוני מייל לדיווח	F6

Activity Diagram:

TCP Capture and Analysis – Real Time Flow



10.2. איסוף מידע וניתוחים סטטיסטיים (אנליטיקות)

ביישום זה, איסוף הנתונים מהווה מרכיב מרכזי לצורך זיהוי אנומליות. קיימים מספר מצבים שבהם ניתן לאסוף נתונים נוספים, וזאת במטרה להבטיח כי הדיווחים למשתמש יהיו מדויקים ומבוססים יותר. הנתונים הרלוונטיים מוצגים בטבלה שלעיל.

סוג מידע	למה הוא חשוב
אחסון ממוצעי שימוש במשאבי מחשב.	הנתונים נאספים באמצעות מנגנון לניטור משאבים (CPU, RAM) אחסון. (הערכים נשמרים במסד הנתונים יחד עם חישוב סטיית תקן, במטרה לאפשר זיהוי אנומליות בשימוש חריג ודיווח מדויק יותר על עומסי יתר. עבור כל משאב מתועדת גם כמות הפעמים שבה המשתמש ביקש לצפות באחוזי השימוש בו, וכן נשמר סכום כלל התוצאות שנמדדו עבור אותו משאב.
נתוני בדיקת קבצים	בעת שהמשתמש מבצע בדיקת קובץ, נשמרים במסד הנתונים שם הקובץ, תאריך הבדיקה ותוצאת הסריקה. שמירה זו מאפשרת למשתמש גישה להיסטוריית הבדיקות לצורך מעקב ובקרה
נתוני דפוסים חשודים	במהלך ניתוח תעבורת הרשת נאספים פקטות (Packets) ומסווגים לפי פרמטרים טכניים כגון: פורטים, פרוטוקולים, ותדירות הופעה. הנתונים נשמרים במסד הנתונים לצורך זיהוי "פטרנים" חשודים, איתור ניסיונות תקיפה, ומתן אפשרות לגישה להיסטוריית התעבורה.
נתוני משתמש	פרטי המשתמשים (דוא"ל, סיסמה מוצפנת) נשמרים במסד הנתונים, כדי לאפשר למערכת לנהל מספר פרופילים. ההצפנה מבטיחה אבטחת מידע ומניעת גישה לא מורשית.

11. תיאור/התייחסות לנושאי אבטחת מידע

הפריטים הרגישים ביותר במערכת הם פרטי המשתמשים, ובעיקר סיסמאות הפרופילים שנוצרו. לשם אבטחתן, מיושמת בצד השרת ספריית Bcrypt.Net המשמשת לביצוע Hashing לסיסמאות ובכך מבטיחה הגנה מפני חשיפה לא מורשית.

12. משאבים הנדרשים לפרויקט:

12.1. מספר שעות המוקדש לפרויקט, חלוקת עבודה בין חברי הצוות

שעות	מטרה
50	איסוף מידע ולימדה על ספריות
100	תכנות צד לקוח client
100	תכנות שרת server
50	בדיקות עבודת שירותי התוכנה

12.2. ציוד נדרש

החומרה הנדרשת עבור הפרויקט :-

- ווינדוז 10 או 11
- מעבד עובד ברמת intel core i3

12.3. תוכנות נדרשות

Visual Studio Code

Dotnet cli

Nodejs

MongoDB Shell

MongoDB Compass

MongoDB Server

PostMan

12.4. ידע חדש שנדרש ללמוד לצורך ביצוע הפרויקט

- **SignalR** ו- **Sockets** - תקשורת דו-כיוונית בזמן אמת וניהול חיבורים.
- **מבנה חבילות רשת** - הכרת שדות TCP/UDP/ICMP לצורך זיהוי התקפות.
- **MailjetAPI** - שליחת מיילים אוטומטיים להתראות ודוחות.
- **VirusTotalAPI** - בדיקת קבצים וקישורים וקבלת תוצאות סריקה.

12.5. ספרות ומקורות מידע

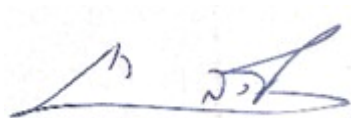
- **PacketDotNet** : ספרייה לפיענוח חבילות (parsing) ושדות כותרת ברמות שונות (Ethernet/IP/TCP/UDP/ICMP) לצורך ניתוח וסיווג פקטות. שימשה לבניית שכבת הפיענוח לפני ההעברה ללוגיקה אנליטית.
- **SharpPcap** : מעטפת לכידת חבילות מרכיב כרטיס הרשת (pcap) כולל פתיחת אינטרפייסים, סינון (BPF) והזרמה בזמן אמת. שימשה לשכבת ה-capture לפני ה-PacketDotNet.
- **Mailjet** : תיעוד ליישום שליחת מיילים טרנזקציוניים/התראות, עבודה עם תבניות ודוחות מצורפים. שימש למימוש התראות ודיווחים למשתמש.

13. תכנית עבודה ושלבנים למימוש הפרויקט

12.2024	קבלת החלטה על נושא הפרויקט והתנעה ראשונית	.1
12.9.2025	כתיבת הצעה/ניתוח פרויקט וממשקים	.2
12.9.2025	Code Review 1 + מסירת ספרי פרויקט	.3
15.10.2025	Code Review 2 – ועדה פנימית (מועד הגנה?)	.4

14. תכנון הבדיקות שיבוצעו

תיאור הבדיקה	התנהגות צפויה
הכנסת פרטי רישום עם מייל תקין וסיסמה חוקית	השרת מחזיר קוד HTTP 200 OK, המשתמש נוסף למסד הנתונים בהצלחה
הכנסת פרטי רישום עם סיסמה לא תקינה (לא עומדת ב־REGEX)	השרת מחזיר קוד HTTP 400 עם הודעת שגיאה על תקינות הסיסמה
בדיקת תגובה לשרת להכנסת נתוני משתמש שכבר קיים	השרת צפוי להחזיר 400 בקשה לא תקינה כי המשתמש אשר הוקלד כבר נמצא
המשתמש מזין קישור זדוני בשדה ולוחץ על הכפתור "Check Url"	מתקבל מייל אוטומטי למשתמש עם דוח סריקה מפורט: שם הדומיין, תאריך ושעה, מספר מנועים שסימנו כ-malicious, מספר מנועים שסימנו כ-harmless/undetected והמלצה לבדוק שוב את המקור, מוצגת גם הודעה בממשק שהקישור מסוכן
המשתמש מזין קישור תקין בשדה ולוחץ על הכפתור "Check Url"	מוצגת בממשק הודעה שהקישור בטוח
המשתמש מזין קישור חשוד בשדה ולוחץ על הכפתור "Check Url"	מתקבל מייל עם דוח סריקה שמציין את מספר המנועים שסימנו כ-Suspicious, מוצגת גם הודעה בממשק שהקישור חשוד
המשתמש מעלה קובץ זדוני דרך "File Checker"	מתקבלת הודעה שהקובץ מסוכן כולל מספר מנועים שזיהו אותו, ונשלח דוח PDF למייל
ברקע: מתבצע ניטור פקטות רשת, מזוהה דפוס התקפה (למשל TCP FLOOD)	הפקטות החשודות מסומנות כחשודות/זדוניות, ומתווספות לדוח פקטות חשודות, ונשלח דוח PDF למייל
ברקע: מתבצע ניטור חומרה, מזוהה שימוש חריג ב- (RAM, DISC, CPU)	נוצר דוח PDF עם נתוני השימוש החריגים ונשלח למייל המשתמש
ברקע: מתקבלות פקטות חדשות מהשרת (SignalR)	הרשימה מתעדכנת אוטומטית ומוצגות הפקטות החדשות
המשתמש לוחץ על כפתור סינון ובוחר "TCP"	ברשימה מוצגות רק פקטות מסוג "TCP"
המשתמש לוחץ על פקטה מסויימת ברשימה	נפתח חלון פרטים עם מידע על הפקטה שנבחרה
המשתמש משנה משנה את הסינון כאשר יש פקטה מסומנת	בחירת הפקטה מתאפסת (החלון נסגר)



חתימת המנחה האישי

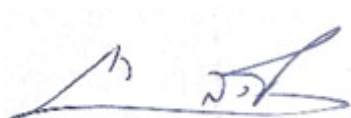


חתימת הסטודנט

א. הערות ראש המגמה במכללה

ב. אישור ראש המגמה

להב רון



תאריך

חתימה

שם

ג. הערות הגורם המקצועי מטעם מה"ט

ד. אישור הגורם המקצועי מטעם מה"ט

שם: _____ חתימה: _____ תאריך: _____