**סטטוס התקדמות והכנה למחר:**

**משימה:**

לעבור על כל מהמאמרים המצטטים את PAC-GPT ו- PCAP-GAN (מ2022) ולבדוק שני סוגים מאמרים:

1. מאמר שפותר את אותה הבעיה (network data flow) עם קוד, שלקח חלקים/ הציע פתרון חדש טוב יותר

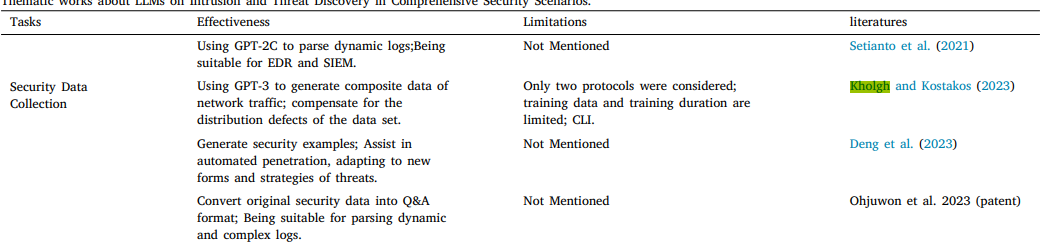
2. 2/3 מאמרים שדנים על אותה בעיה בתחום - אותם אפשר לקחת ולעשות review (כפי שאמרנו מדובר בפרויקט לא פשוט).

**תהליך העבודה:**

1. עברנו על כל המאמרים המצטטים (קיימים מאמרים חופפים, אבל זה לפי דעתי רק 2). קראנו את הABSTRACT וסיכמנו במה עוסק המאמר, מה ה"חידוש" ובנוסף הסתכלנו באיזה רמה הוזכר המאמר המצוטט ועד כמה הוא רלוונטי. על בסיס זה ייצרנו משפך ופילטרנו את המאמרים הלא רלוונטים.

2. עברנו על המאמרים שנראו לנו יותר רלוונטיים, ושעסקו במאמר בצורה משמעותית.

**ממצאים:**

1. לגבי PAC-GPT -:
   1. מצאנו את המאמר **TrafficGPT: Breaking the Token Barrier for Efficient Long Traffic Analysis and Generation** שהיה נראה די רציני (ככה היה נראה לנו לפחות אבל לא מספיק העמקנו בו עדיין).
   2. לפי האתרhttps://paperswithcode.com/ אין קוד למאמר. בנוסף מנסיונות חיפוש נוספים באינטרנט הגענו לפרויקט TrafficGPT אחר (ממה שקראנו לפחות בabstract הוא פחות רלוונטי ומתעסק ליטרלי בtraffic data. כלומר כבישים/רמזורים וכאלה).
   3. בנוסף באחד ממאמרי ה-REVIEW ראינו השוואה בין המאמר המקורי (PAC-GPT) למאמרים נוספים (שם המאמר **A survey of large language models for cyber threat detection**). 
2. לגבי PCAP GAN
   1. פה טרם הספקנו לעבור על כל המאמרים אבל כן מצאנו מאמר שמדבר על גנרוט של  
       IP HEADERאבל trace ולא flow.
   2. שם המאמר - **Practical GAN-based Synthetic IP Header Trace Generation using NetShare**
   3. יש קוד, נמצא כאן [GitHub - netsharecmu/NetShare: (SIGCOMM '22) Practical GAN-based Synthetic IP Header Trace Generation using NetShare](https://github.com/netsharecmu/NetShare)
   4. פה השאלה העיקרית שאנחנו מנסות להבין, ונשמח לעזרתכם בזה היא להבין האם ניתן לייצר framework דומה רק על flow.
   5. ואז זה יחסית מתקשר ל- PAC-GPT

**סיכום:**

נשמח לשמוע את דעתכם על הכיוונים שמצאנו (איך שהם נשמעים לכם כרגע לפחות).  
אם אהבתם את הכיוונים שמצאנו, ונראה לכם שזה משהו ששווה להתקדם איתו, נשמח לדעת.  
  
אתגרים שנתקלנו בהם ונשמח לסיוע:

1. לעזור לנו למצוא קוד של **TrafficGPT**
2. להבין האם המאמרים הבאים מתאימים לסוג פרויקט של review והשוואה:
   1. PAC-GPT (מצורף)
   2. GPT-2C: A GPT-2 parser for Cowrie honeypot logs (מצורף)
   3. PENTESTGPT: Evaluating and Harnessing Large Language Models for Automated Penetration Testing (מצורף)
   4. Ohjuwon et al. 2023 (patent)   
      רשום במאמר שזה פטנט, ובאמת לא היה קישור למאמר עצמו.. זה אומר שאי אפשר להשיג אותו?
3. לעזור לנו להבין האם ניתן להמיר את Netshare ל- Flow ואז זה יכול להתקשר ל PAC-GPT.