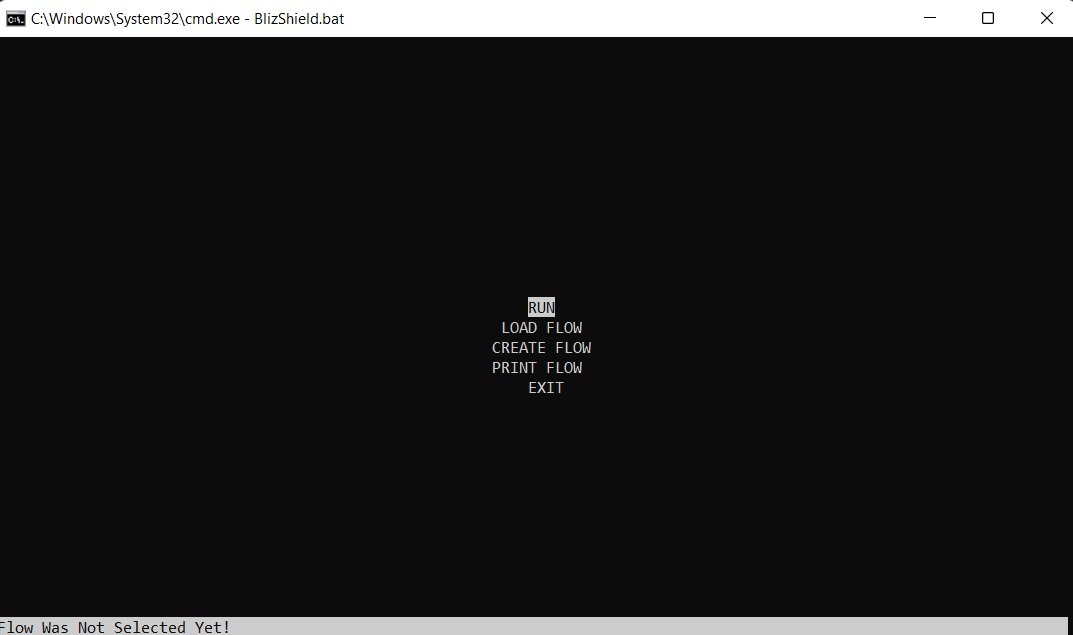
# סדנא – פרוייקט BlizShield

BlizShield – זוהי תוכנית שמביאה למשתמש מקום יחיד לניתוח איומי בטיחות על רשת מסוימת. בתוכנה שמים דגש על גנריות ועל יכולתה לגדול בעתיד, לכן היא מחולקת ל-3 חלקים עיקריים:

1. Plugins/פלאגינים – כל פלאגין, היא תוכנית עצמאית ש-BlizShield מריצה. משתמשים יכולים להוסיף פלאגינים כרצונם וכך להגדיל את "הפעולות" ש-BlizShield יודע לעשות.
2. Exporters/מייצאים – אנחנו מספקים מספר אפשרויות כדי לייצא את המידע הנאסף. המשתמש יכול לבחור כיצד הוא יירצא לייצא את המידע ולמעשה "יחסית" בקלות ניתן להוסיף "מייצאים" חדשים. כרגע, קיימים בפרוייקט 2 מייצאים: ייצוא לקובץ וייצוא ל-Elastic.
3. Flow/תרשים זרימה – BlizShield היא תוכנית דינמית ולמעשה אינה יודעת מה לעשות ומה להריץ. היא מצפה לקבל מהמשתמש תרשים זרימה אשר יגדיר לה איך להריץ את הפלאגינים ולאן לייצא את הנתונים. כיום, בעזרת ה-TUI שיצרנו, ניתן ליצור תרשים זרימה חדש או להשתמש באחד קיים שאנחנו מספקים עם המערכת.

כעת, אחרי שראינו את שלושת החלקים העיקריים של BlizShield – ניתן להבין כי BlizShield יכולה לשמש בפוטנציאל כעטיפה חכמה לכמעט כל פרויקט שתרצו. לכל פרוייקט כזה, נצטרך ליצור פלאגין ולהוסיף אותו לתרשים הזרימה.

## איך להריץ?

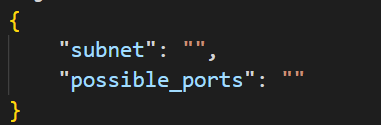
1. יש להוריד את הפרוייקט על ידי הורדת ה-REPO מ-GITHUB או על ידי הורדת Release ZIP
2. במערכת ווינדוס – יש להריץ BlizShield.bat  
   
3. יש לבחר LOAD FLOW כדי לטעון תרשים זרימה *(בכדי ליצור תרשים זרימה חדש – רדו למטה בקובץ זה)*
4. בחרו את תרשים הזרימה שתרצו להריץ (מתרשימי הזרימה הקיימים)
5. בחרו YES לאישור סופי
6. וזהו! כעת, התרשים טעון למערכת ונשאר רק להריץ אותו על ידי בחירת האפשרות RUN.

## יצירת תרשים זרימה חדש

1. יש ללחוץ על CREATE FLOW
2. יש לבחור פלאגין על ידי לחיצה על ADD PLUGIN
3. בחרו את הפלאגין שתרצו להוסיף לתרשים
   1. מלאו את פרטי הקונפיגורציה של הפלאגין
   2. שימו ♥: כדאי ששם הפלאגין יהיה ייחודי
4. בחרו כיצד תרצו להריץ את הפלאגין:
   1. PARALLEL – ריצה במקביל – בזמן ריצת תרשים הזרימה, פלאגין זה ירוץ במקביל לשאר הפלאגינים בתהליך חדש וללא שום מגבלות עליו
   2. SEQUANTIAL – ריצה אחרי פלאגין אחר
      1. כעת, תצטרכו לבחור אחרי איזה פלאגין תרצו להריץ את הפלאגין הזה מהפלאגינים הקיימים בתרשים הזרימה
      2. וכעת, יש לבחור כיצד תרצו שהוא ירות
         1. RUN ANYWAY – הפלאגין החדש ירוץ בכל מקרה, אבל אחרי הפלאגין הקודם שנבחר.
         2. RUN ONLY IF STATUS IS TRUE – הפלאגין החדש ירוץ רק אם הפלאגין הקודם החזיר תוצאה חיובית
         3. RUN ONLY IF STATUS IS FALSE – הפלאגין החדש ירוץ רק אם הפלאגין הקודם החזיר תוצאה שלילית
5. חזרו על השלבים 2-4 כדי להוסיף עוד פלאגינים
6. בסיום בחרו SAVE ותנו שם לתרשים הזרימה החדש שלכם
7. התרשים יטען למערכת ויהיה ניתן להשתמש בו מיד על ידי לחיצה על RUN

## יצירת פלאגין חדש

יצירת פלאגין חדש נעשת במספר שלבים טכניים. יש לעקוב אחריהם במדויק.

1. יש ליצור תקיה חדשה תחת הנתיב Clients\Plugins\Python
   1. שימו ♥ - כרגע אנחנו מאפשרים להריץ פלאגינים רק בפייתון, בעתיד, התשתית מאפשרת להוסיף אופציות הרצה נוספות!
2. שם התיקייה הוא שם הפלאגין שלכם
3. בתיקייה זו, צריכים להיות 3 קבצים:
   1. \_\_init\_\_.py – קובץ ריק – הוא שם רק בשביל הקונבציה של פייתון.
   2. config.json – קובץ בפורמט JSON שמגדיר את הקונפיגורציה שהפלאגין שלכם אמור לקבל. ככה כשיוצרים תרשים זרימה, BlizShield ידע, איזה קונפיגורציה הוא צריך למלא.  
      דוגמא:  
      
   3. main.py – קובץ זה הוא הקובץ ש-BlizShield יריץ כשיקרא הפלאגין. בקובץ זה צריכה להיות פונקציה בשם run שמקבלת מילון (תצפו שהוא יהיה כמו שהוגדר בקובץ config.json) והפונקציה צריכה להחזיר רשימה של מילונים עם תוצאות הריצה
      1. מומלץ שכל תוצאה תכיל ערך status מסוג Bool!
4. זהו, נותר רק לממש את הלוגיקה שברצונכם להריץ בפלאגין והוא עכשיו קיים במערכת!