

# פרויקט: מנתח לוגים של תעבורת רשת

שלב 2 - בניית מילונים

## מטרת השלב

בשלב הקודם למדנו לסנן ולחלץ נתונים מהלוג. בשלב זה נארגן את הנתונים במילונים כדי לאפשר גישה מהירה וניתוח יעיל. נשתמש ב-**Dict Comprehension** ליצירת מילונים בצורה קצרה ויעילה.

## דרישות שלב 2

לכל דרישה יש לכתוב פונקציה נפרדת.

### 1 ספירת פניות לפי IP

כתבו פונקציה שמקבלת את הנתונים ומחזירה מילון: כתובת IP מקור → מספר הפניות שלה.

דוגמה לפלט:

```
{ "192.168.1.100": 156, "45.33.32.156": 23,  
  "10.0.0.50": 89 }
```

## 2 מיפוי פורט לפרוטוקול

כתבו פונקציה שמקבלת את הנתונים ומחזירה מילון: מספר פורט → שם הפרוטוקול.

### דוגמה לפלט:

```
{ 443: "HTTPS", 80: "HTTP", 22: "SSH" }
```

## 3 זיהוי חשדות לכל IP

כתבו פונקציה שמקבלת את הנתונים ומחזירה מילון: כתובת IP → רשימת סוגי החשדות שלה.

הפונקציה תבדוק את 4 סוגי החשדות שהגדרנו:

- EXTERNAL\_IP - כתובת חיצונית
- SENSITIVE\_PORT - פורט רגיש (22, 23, 3389)
- LARGE\_PACKET - חבילה מעל 5000 בייט
- NIGHT\_ACTIVITY - פעילות בין 00:00 ל-06:00

### דוגמה לפלט:

```
{ "45.33.32.156": ["EXTERNAL_IP", "LARGE_PACKET"],  
  "87.120.5.22": ["EXTERNAL_IP", "NIGHT_ACTIVITY",  
  "SENSITIVE_PORT"], "203.0.113.50": ["EXTERNAL_IP"] }
```

## 4 סינון מילון החשדות

כתבו פונקציה שמקבלת את מילון החשדות ומחזירה מילון חדש רק עם כתובות שיש להן לפחות 2 סוגי חשדות.

IP עם חשד אחד עדיין יכול להיות תקין. IP עם כמה חשדות יחד - סביר יותר שמדובר באיום אמיתי.

**זכרו:** המבנה צריך להיות דינאמי. כשנוסיף סוג חשד חמישי או שישי בעתיד, השינוי בקוד צריך להיות מינימלי.