פרויקט: מנתח לוגים של תעבורת רשת

שלב 3 - Lambda, Map ו-Filter

מטרת השלב

בשלב זה נלמד לכתוב קוד קצר ויעיל יותר באמצעות:

- **Lambda** - פונקציות קצרות בשורה אחת
- **Map** - הפעלת פונקציה על כל איבר ברשימה
- **Filter** - סינון רשימה לפי תנאי

נשתמש בכלים אלה כדי לעבד ולסנן את נתוני הלוג.

דרישות שלב 3

לכל דרישה יש להשתמש ב-Lambda, Map ו/או Filter.

1 חילוץ שעה מ-timestamp

באמצעות `map` ו- `lambda` , צרו רשימה של השעות בלבד (מספר 0-23) מכל השורות.

דוגמה:

```
# קלט (timestamps): ["2024-01-15 08:23:45", "2024-01-15 14:30:00", "2024-01-15 02:15:30"] # פלט: [8, 14, 2]
```

2 המרת גודל חבילות

באמצעות `map` ו- `lambda` , המירו את גודל כל החבילות מבייטים לקילובייט (חלקו ב-1024).

דוגמה:

```
# קלט (bytes): [1024, 2048, 5120] # פלט (KB): [1.0, 2.0, 5.0]
```

3 סינון שורות לפי פורט

באמצעות `filter` ו- `lambda` , סננו רק שורות עם פורט רגיש (22, 23, או 3389).

דוגמה:

```
קלט - כל השורות # פלט - רק שורות עם פורט 22, 23 או # 3389
```

4 סינון פעילות לילה

באמצעות `filter` ו- `lambda` , סננו רק שורות שהפעילות בהן התרחשה בשעות 00:00-06:00.

5 מילון בודקי חשדות

צרו מילון שבו המפתח הוא שם החשד והערך הוא פונקציית `lambda` שבודקת אם שורה מתאימה לחשד.

דוגמה למבנה:

```
suspicion_checks = { "EXTERNAL_IP": lambda row: ...,
"SENSITIVE_PORT": lambda row: ..., "LARGE_PACKET":
lambda row: ..., "NIGHT_ACTIVITY": lambda row: ... }
```

> מבנה זה מאפשר להוסיף סוגי חשדות חדשים בקלות - פשוט מוסיפים שורה למילון.

6 הפעלת בדיקות על שורה

כתבו פונקציה שמקבלת שורה ואת מילון הבודקים, ומחזירה רשימה של כל החשדות שהשורה מתאימה להם. השתמשו ב-`filter` כדי לסנן רק את הבדיקות שעברו.

דוגמה:

```
# קלט: row = ["2024-01-15 03:23:45", "45.33.32.156",
"10.0.0.5", "22", "SSH", "6000"] # פלט: ["EXTERNAL_IP",
"SENSITIVE_PORT", "LARGE_PACKET", "NIGHT_ACTIVITY"]
```

7 עיבוד כל הלוג

באמצעות `map`, הפעילו את פונקציית הבדיקה על כל שורות הלוג. לאחר מכן, באמצעות `filter`, סננו רק שורות שיש להן לפחות חשד אחד.

יתרון המבנה הדינאמי: כשנרצה להוסיף סוג חשד חדש (למשל `FREQUENT_ACCESS`), נצטרך רק להוסיף שורה אחת למילון הבודקים - שאר הקוד יעבוד אוטומטית.