

פרויקט: מנהל לוגים של תעבורת רשת

המשימה

יחידת המודיעין קיבלה קובץ לוג ענק - אלף רשומות של תעבורת רשת מהשבועות האחרונות. יש חשד שאורם עיון מנסה לחדר למערכת. המשימה שלכם: לבנות מערכת אוטומטית שתסרוק את הנתונים, תזהה דפוסים חשודים, ותיצור דוח מסודר עם כל האינזים הפוטנציאליים. הזמן לוחץ - אי אפשר לעبور ידנית על 10,000 שורות. אתם צריכים קוד חכם שיעשה את העבודה.

רकע: מה זה פורט?

כשמחשב מתקשר עם מחשב אחר, הוא צריך לדעת לאיזה "שירות" לפנות. **פורט** הוא מספר (0-65535) שמצויה את השירות. דמיינו בנין משרד: כתובת ה-IP היא כתובות הבניין, והפורט הוא מספר החדר.

שימוש	שירות	פורט
אתרי אינטרנט	HTTP	80
אתרים מאובטחים	HTTPS	443
שליטה מרוחק (מסוקן)	SSH	22
שליטה במחשב Windows	RDP	3389

מבנה הקבצים

```
log_analyzer/
├── main.py
├── config.py
├── reader.py
├── checks.py
└── analyzer.py
```

נקודות כניסה - מפעיל את התוכנית #
הADRות (פורטים רגילים, ספויים) #
קריאת קובץ הלוג #
פונקיות בדיקת שחזור #
ויתוח ויזיה חשודים #

```
|__ reporter.py      יצירת דוחות #
└__ network_traffic.log קובץ הנתונים #
```

דרישות עבודה עם Git

חשוב: כל פקודות Git יבוצעו בטרמינל בלבד - לא ב-GitKraken או כלים ויזואליים אחרים.

מבנה Git יבוצעו בטרמינל בלבד - לא ב-GitKraken או כלים ויזואליים אחרים.

סדר העבודה:

```
git checkout -b stage-1      חדש branchفتح # ... כתיבת פונקציה ...
git add .                    #
git commit -m "add load_csv function"
... כתיבת פונקציה נוספת ...
git commit -m "add filter_external_ips"
git push origin stage-1    בסיום שלב #
                           # מיזוג ל-main וpush PRفتح #
```

מתי לעשות Commit: אחרי כל פונקציה שעבדה ונבדקה.

מתי לעשות PR: בסיום כל שלב, לפני מעבר לשלב הבא.

דרישות קוד

- **חלוקת לפונקציות:** כל משימה = פונקציה נפרדת. פונקציה עשו דבר אחד.
- **שמות ברורים:** filter_by_port ולא f1
- **לא קוד גלובלי:** כל הקוד בתוך פונקציות, הפעלה דרך main().
- **אבל -** אחרי כתיבת כל פונקציה, בידקו אותה! כתבו קריאה זמנית לפונקציה, ודאו שהיא עובדת, ורק אז עשו commit ומחקו את הקוד הבדיקה.