Розширена робота з БД - Система логування подій (опціонально)

Інструменти

1. Обліковий запис на github
2. Встановлена IDE для розробки на python, наприклад pycharm.
3. Sqlite browser для перегляду структури БД - https://sqlitebrowser.org/
4. Для виконання завдання потрібно буде розібратися з SQL Foreign Keys, приклади:
    a. https://www.sqlitetutorial.net/sqlite-foreign-key/
    b. https://www.youtube.com/watch?v=FrTQSPSbVC0

Завдання

1. За допомогою Python створіть БД sqlite3 та наступні таблиці:
    a. EventSources (ДжерелаПодій). Структуратаблиці:
        i. id (PRIMARY KEY, INTEGER)
        ii. name (TEXT, UNIQUE) - Назва джерела (наприклад, "Firewall_A", "Web_Server_Logs", "IDS_Sensor_B")
        iii. location (TEXT) - Місце розташування/IP джерела
        iv. type (TEXT) - Тип джерела (наприклад, "Firewall", "Web Server", "IDS")
    b. EventTypes (ТипиПодій):
        i. id (PRIMARY KEY, INTEGER)
        ii. type_name (TEXT, UNIQUE) - Назва типу події (наприклад, "Login Success", "Login Failed", "Port Scan Detected", "Malware Alert")
        iii. severity (TEXT) - Серйозність типу події (наприклад, "Informational", "Warning", "Critical")
    c. SecurityEvents (ПодіїБезпеки):
        i. id (PRIMARY KEY, INTEGER)
        ii. timestamp (DATETIME) - Час події
        iii. source_id (INTEGER, FOREIGN KEY до EventSources.id)
        iv. event_type_id (INTEGER, FOREIGN KEY до EventTypes.id)
        v. message (TEXT) - Повний текст логу/повідомлення
        vi. ip_address (TEXT, NULLABLE) - IP-адреса, пов'язана з подією (якщо є)
        vii. username (TEXT, NULLABLE) - Ім'я користувача, пов'язане з подією (якщо є)
2. Внесіть наступні дані до таблиці EventTypes:

Event type_name	**Event severity**
Login Success	Informational
Login Failed	Warning

Port Scan Detected	Warning
Malware Alert	Critical

3. Внесіть декілька тестових значень у таблицю EventSources та 10+ тестових значеньдо таблиці SecurityEvents
4. Розробіть програму на python, яка містить у собі наступні функції:
    a. Функція для реєстрації нового джерела подій.
    b. Функція для реєстрації нового типу подій.
    c. Функція для запису нової події безпеки (з автоматичним заповненням timestamp).
    d. Функції запиту даних:
        i. Отримати всі події "Login Failed" за останні 24 години.
        ii. Виявити IP-адреси, з яких було більше 5 невдалих спроб входу за 1 годину (потенційна атака підбору пароля).
        iii. Отримати всі події з рівнем серйозності "Critical" за останній тиждень, згруповані за джерелом.
        iv. Знайти всі події, що містять певне ключове слово у повідомленні (message).
5. Завантажити виконане завдання та файл БД на персональний github