SQL Task

1)Create a Database

```
CREATE DATABASE cyber_security_db;
```

Purpose: Every project starts by organizing data inside a database.

2)Create a Table for User Logins

```
CREATE TABLE user_logins (
   id INT PRIMARY KEY AUTO_INCREMENT,
   username VARCHAR(50),
   login_time DATETIME,
   status VARCHAR(10)
);
```

Purpose: Store login activity data — useful for detecting failed attempts.

3)Insert Data into the Table

```
INSERT INTO user_logins (username, login_time, status)
VALUES
('user1', NOW(), 'success'),
('user2', NOW(), 'failed'),
('user3', NOW(), 'failed');
```

Purpose: Practice data entry for system logs.

4) Display All Records

```
SELECT * FROM user_logins;
```

Purpose: View all stored login activities.

5) Filter Failed Logins

```
SELECT username, login_time
FROM user_logins
WHERE status = 'failed';
```

Purpose: Identify suspicious users — simple log monitoring.

6) Count Total Failed Logins

```
SELECT COUNT(*) AS failed_attempts
FROM user_logins
WHERE status = 'failed';
```

Purpose: Helps in calculating basic threat metrics.

7) Update a Record (Fix a Mistake)

```
UPDATE user_logins
SET status = 'success'
WHERE username = 'user2';
```

Purpose: Learn to correct or modify stored data.

8) Delete Old Records

```
DELETE FROM user_logins
WHERE login_time < '2025-10-01';
```

Purpose: Data cleanup — important for database maintenance.

9) Sort Records by Time

```
SELECT *
FROM user_logins
ORDER BY login_time DESC;
```

Purpose: See the latest activities first — like a security dashboard.

10) Join with Another Table (Threat Info)

```
CREATE TABLE threat_reports (
   report_id INT PRIMARY KEY AUTO_INCREMENT,
   username VARCHAR(50),
   threat_type VARCHAR(50),
   severity VARCHAR(10)
);

SELECT u.username, u.status, t.threat_type, t.severity
FROM user_logins u
JOIN threat_reports t
```

ON u.username = t.username;

Purpose: Combine login data with detected threats — key concept in cyber log analytics.