

Infosys Springboard 6.0

SQL Task

1. Introduction to SQL

SQL (Structured Query Language) is used to manage and analyze data in relational databases. In cybersecurity analytics, SQL helps in storing, querying, and filtering network logs for anomaly detection.

2. Database and Table Management

```
CREATE DATABASE cyber_security;
USE cyber_security;
CREATE TABLE network_logs (id INT PRIMARY KEY, src_ip VARCHAR(50), dest_ip
VARCHAR(50), protocol VARCHAR(10), threat_level VARCHAR(20));
SHOW TABLES;
DESCRIBE network_logs;
```

3. CRUD Operations

```
INSERT INTO network_logs VALUES (1, '192.168.1.10', '10.0.0.5', 'TCP', 'Low');
UPDATE network_logs SET threat_level = 'High' WHERE id = 1;
DELETE FROM network_logs WHERE id = 3;
SELECT * FROM network_logs;
```

4. Filtering and Sorting

```
SELECT * FROM network_logs WHERE protocol = 'TCP';
SELECT src_ip, COUNT(*) AS attack_count FROM network_logs GROUP BY src_ip ORDER BY
attack_count DESC;
```

5. Aggregate Functions and Grouping

```
SELECT COUNT(*) AS total_logs FROM network_logs;
SELECT protocol, AVG(packet_size) FROM traffic_data GROUP BY protocol;
```

6. SQL Joins

```
SELECT n.src_ip, t.threat_type FROM network_logs n INNER JOIN threat_types t ON n.id =
t.log_id;
```

7. Subqueries and Views

```
CREATE VIEW high_threats AS SELECT * FROM network_logs WHERE threat_level = 'High';
SELECT * FROM high_threats;
DROP VIEW high_threats;
```

8. Indexes and Constraints

```
CREATE INDEX idx_protocol ON network_logs(protocol);
ALTER TABLE network_logs ADD CONSTRAINT chk_threat CHECK (threat_level IN ('Low',
'Medium', 'High'));
DROP INDEX idx_protocol ON network_logs;
```

9. Conclusion

SQL ensures structured data handling, helping in efficient retrieval of network log information and seamless integration with Python for AI-based cyber threat analysis.