**TABLE CREATION**

CREATE TABLE ATTACK\_TYPE (

ATTACK\_TYPE\_ID VARCHAR(20) NOT NULL,

TYPE\_NAME VARCHAR(50) NOT NULL,

CONSTRAINT ATTACK\_TYPE\_PK PRIMARY KEY (ATTACK\_TYPE\_ID));

CREATE TABLE ORGANIZATION (

ORG\_ID VARCHAR(20) NOT NULL,

ORG\_NAME VARCHAR(100) NOT NULL,

LOCATION VARCHAR(100),

CONSTRAINT ORGANIZATION\_PK PRIMARY KEY (ORG\_ID));

CREATE TABLE THREAT (

THREAT\_ID INT NOT NULL,

THREAT\_NAME VARCHAR(100) NOT NULL,

SEVERITY\_LEVEL VARCHAR(20),

DATE\_OCCURRED DATE,

ATTACK\_TYPE\_ID INT,

CONSTRAINT THREAT\_PK PRIMARY KEY (THREAT\_ID),

CONSTRAINT THREAT\_FK\_ATTACK\_TYPE FOREIGN KEY (ATTACK\_TYPE\_ID) REFERENCES ATTACK\_TYPE(ATTACK\_TYPE\_ID));

CREATE TABLE INCIDENT\_RESPONSE\_TEAM (

TEAM\_ID VARCHAR(20) NOT NULL,

TEAM\_NAME VARCHAR(100) NOT NULL,

CONTACT\_INFO VARCHAR(100),

CONSTRAINT INCIDENT\_RESPONSE\_TEAM\_PK PRIMARY KEY (TEAM\_ID));

CREATE TABLE THREAT\_SOURCE (

SOURCE\_ID VARCHAR(20) NOT NULL,

SOURCE\_TYPE VARCHAR(50) NOT NULL,

SOURCE\_DESCRIPTION TEXT,

CONSTRAINT THREAT\_SOURCE\_PK PRIMARY KEY (SOURCE\_ID));

CREATE TABLE MITIGATION\_ACTION (

MITIGATION\_ID VARCHAR(20) NOT NULL,

ACTION\_DESCRIPTION VARCHAR(255) NOT NULL,

DATE\_IMPLEMENTED DATE,

CONSTRAINT MITIGATION\_ACTION\_PK PRIMARY KEY (MITIGATION\_ID));

CREATE TABLE THREAT\_IMPACT (

THREAT\_ID INT,

ORG\_ID VARCHAR(20),

IMPACT\_LEVEL VARCHAR(50),

IMPACT\_DATE DATE,

PRIMARY KEY (THREAT\_ID, ORG\_ID),

FOREIGN KEY (THREAT\_ID) REFERENCES THREAT(THREAT\_ID),

FOREIGN KEY (ORG\_ID) REFERENCES ORGANIZATION(ORG\_ID));

CREATE TABLE THREAT\_MITIGATION (

THREAT\_ID INT NOT NULL,

MITIGATION\_ID VARCHAR(20) NOT NULL,

MITIGATION\_STATUS VARCHAR(50),

REVIEW\_DATE DATE,

CONSTRAINT THREAT\_MITIGATION\_PK PRIMARY KEY (THREAT\_ID, MITIGATION\_ID),

CONSTRAINT THREAT\_MITIGATION\_FK\_THREAT FOREIGN KEY (THREAT\_ID) REFERENCES THREAT(THREAT\_ID),

CONSTRAINT THREAT\_MITIGATION\_FK\_MITIGATION FOREIGN KEY (MITIGATION\_ID) REFERENCES MITIGATION\_ACTION(MITIGATION\_ID));

**INSERT STATEMENTS**

INSERT INTO ATTACK\_TYPE (ATTACK\_TYPE\_ID, TYPE\_NAME) VALUES

('AT01', 'Phishing'),

('AT02', 'Malware'),

('AT03', 'Ransomware'),

('AT04', 'DDoS Attack'),

('AT05', 'Spyware'),

('AT06', 'Insider Threat'),

('AT07', 'SQL Injection'),

('AT08', 'Zero-Day Exploit');

INSERT INTO ORGANIZATION (ORG\_ID, ORG\_NAME, LOCATION) VALUES

('ORG001', 'TechCorp', 'New York'),

('ORG002', 'HealthInc', 'Los Angeles'),

('ORG003', 'EduNet', 'Chicago'),

('ORG004', 'BankSecure', 'San Francisco'),

('ORG005', 'RetailHub', 'Seattle'),

('ORG006', 'AutoDrive', 'Detroit'),

('ORG007', 'PharmaMed', 'Boston'),

('ORG008', 'EnergyGrid', 'Houston');

INSERT INTO THREAT (THREAT\_ID, THREAT\_NAME, SEVERITY\_LEVEL, DATE\_OCCURRED, ATTACK\_TYPE\_ID) VALUES

(101, 'Data Breach', 'High', '2024-01-15', 'AT01'),

(201, 'System Infection', 'Medium', '2024-02-20', 'AT02'),

(301, 'Ransom Attack', 'Critical', '2024-03-10', 'AT03'),

(401, 'Website Outage', 'Low', '2024-04-01', 'AT04'),

(501, 'Data Exfiltration', 'High', '2024-05-12', 'AT05'),

(601, 'Unauthorized Access', 'Medium', '2024-06-07', 'AT06'),

(701, 'Database Corruption', 'Critical', '2024-07-15', 'AT07'),

(801, 'Unknown Exploit', 'Critical', '2024-08-22', 'AT08');

INSERT INTO INCIDENT\_RESPONSE\_TEAM (TEAM\_ID, TEAM\_NAME, CONTACT\_INFO) VALUES

('IRT01', 'Alpha Team', 'alpha@response.com'),

('IRT02', 'Bravo Squad', 'bravo@response.com'),

('IRT03', 'Charlie Unit', 'charlie@response.com'),

('IRT04', 'Delta Force', 'delta@response.com'),

('IRT05', 'Echo Crew', 'echo@response.com'),

('IRT06', 'Foxtrot Command', 'foxtrot@response.com'),

('IRT07', 'Golf Squad', 'golf@response.com'),

('IRT08', 'Hotel Division', 'hotel@response.com');

INSERT INTO THREAT\_SOURCE (SOURCE\_ID, SOURCE\_TYPE, SOURCE\_DESCRIPTION) VALUES

('SRC001', 'External', 'Originates from outside the organization'),

('SRC002', 'Internal', 'Originates from within the organization'),

('SRC003', 'Third-Party', 'Supplied by external vendors'),

('SRC004', 'Partner', 'Threat originates from business partners'),

('SRC005', 'Cloud', 'Threat arises from cloud services'),

('SRC006', 'Unknown', 'Source is unidentified'),

('SRC007', 'Nation-State', 'Government-backed threat actors'),

('SRC008', 'Hacktivist', 'Political or social activism threats');

INSERT INTO MITIGATION\_ACTION (MITIGATION\_ID, ACTION\_DESCRIPTION, DATE\_IMPLEMENTED) VALUES

('MA01', 'Apply Patch', '2024-01-16'),

('MA02', 'Isolate Affected Systems', '2024-02-22'),

('MA03', 'Pay Ransom', '2024-03-12'),

('MA04', 'Upgrade Firewall', '2024-04-05'),

('MA05', 'Conduct Audit', '2024-05-15'),

('MA06', 'Reset Credentials', '2024-06-10'),

('MA07', 'Monitor Traffic', '2024-07-18'),

('MA08', 'Deploy Backup', '2024-08-25');

INSERT INTO THREAT\_IMPACT (THREAT\_ID, ORG\_ID, IMPACT\_LEVEL, IMPACT\_DATE) VALUES

(101, 'ORG001', 'Critical', '2024-01-16'),

(201, 'ORG002', 'Moderate', '2024-02-23'),

(301, 'ORG003', 'Severe', '2024-03-13'),

(401, 'ORG004', 'Low', '2024-04-10'),

(501, 'ORG005', 'High', '2024-05-20'),

(601, 'ORG006', 'Moderate', '2024-06-15'),

(701, 'ORG007', 'Critical', '2024-07-25'),

(801, 'ORG008', 'Severe', '2024-08-30');

INSERT INTO THREAT\_MITIGATION (THREAT\_ID, MITIGATION\_ID, MITIGATION\_STATUS, REVIEW\_DATE) VALUES

(101, 'MA01', 'Completed', '2024-01-20'),

(201, 'MA02', 'In Progress', '2024-02-25'),

(301, 'MA03', 'Pending', NULL),

(401, 'MA04', 'Completed', '2024-04-15'),

(501, 'MA05', 'Pending', NULL),

(601, 'MA06', 'Completed', '2024-06-18'),

(701, 'MA07', 'In Progress', '2024-07-28'),

(801, 'MA08', 'Pending', NULL);

**TABLES – Screenshots**

**Attack\_Type**

A screenshot of a computer

Description automatically generated

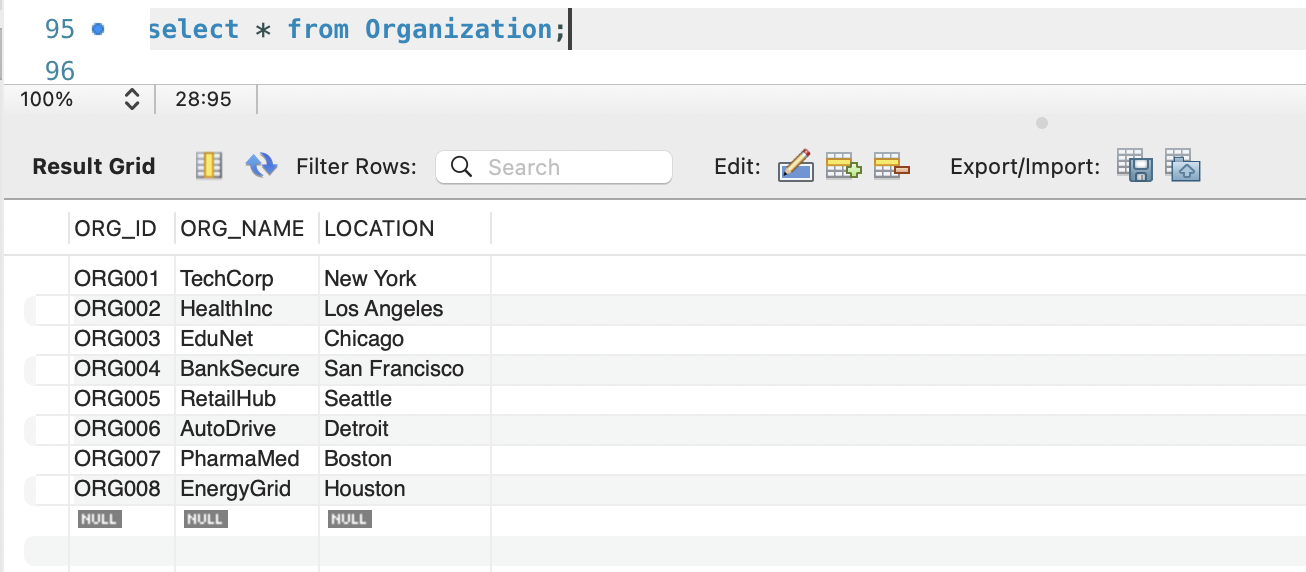
A screenshot of a computer

Description automatically generated

**Organization**

A screenshot of a computer

Description automatically generated



**Threat**

A screenshot of a search engine

Description automatically generated

A screenshot of a computer

Description automatically generated

**Incident\_response\_team**

A screenshot of a computer

Description automatically generated

**Threat\_source**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Mitigation Action**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Threat\_Impact**

A screenshot of a computer

Description automatically generated

A screenshot of a data

Description automatically generated

**Threat\_Mitigation**

A screenshot of a computer

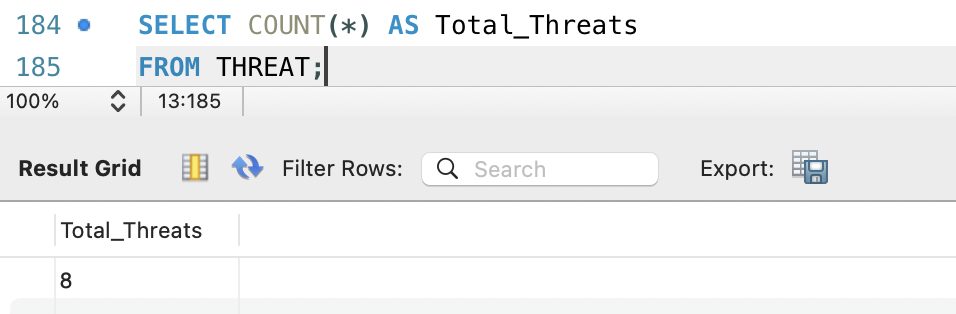
Description automatically generated

A screenshot of a computer

Description automatically generated

**QUERIES**

1. Display the total number of threats recorded in the system.



1. List Threats and Their Corresponding Attack Types

A screenshot of a computer

Description automatically generated

1. What threats impact organizations with a "High" severity level.

A screenshot of a computer program

Description automatically generated

1. Show the number of threats associated with each attack type.

A screenshot of a computer

Description automatically generated

1. Display the mitigation status of threats along with the associated mitigation actions.

A screenshot of a computer

Description automatically generated

1. What are the severity levels by threat source, display the total threats by source and the percentage of critical threats.

A screenshot of a computer

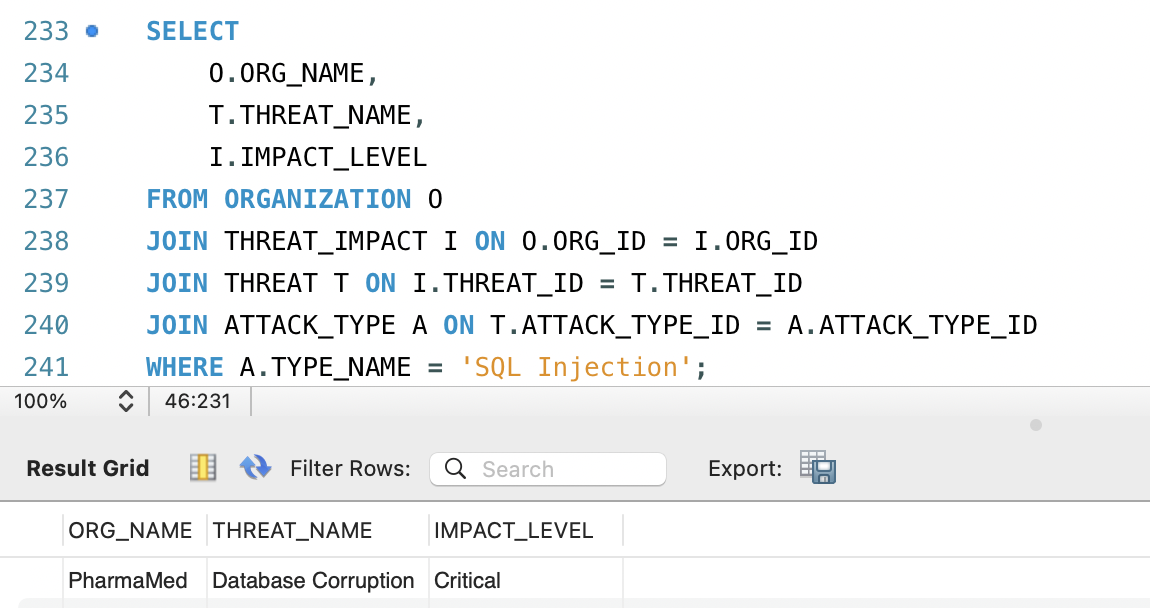
Description automatically generated

1. Filter threats with a severity level of "High" or "Critical."

A screenshot of a computer

Description automatically generated

1. Display organizations impacted specifically by SQL Injection threats.



1. Identify the most common attack type in high-severity threats.

A screenshot of a computer program

Description automatically generated

1. Provide details of threats with completed mitigation actions.

A screenshot of a computer program

Description automatically generated

1. Show all threats, including those without matching attack types.

A screenshot of a computer

Description automatically generated

1. identify the organization most frequently impacted by high-impact threats

A screenshot of a computer program

Description automatically generated

1. Display the total number of threats for each severity level.

A screenshot of a computer

Description automatically generated

1. Show the average number of threats impacting each organization.

A screenshot of a computer

Description automatically generated

1. Which organizations that have not been impacted by any threats.

A screenshot of a computer

Description automatically generated

1. What threats were mitigated after their occurrence date.

A screenshot of a computer program

Description automatically generated

1. List organizations and how many threats have impacted them.

A screenshot of a computer

Description automatically generated

1. Show organizations in New York and the threats that have impacted them

A screenshot of a computer

Description automatically generated

1. Which threats that have been mitigated but not yet reviewed

A screenshot of a computer program

Description automatically generated

1. Display the names of threats along with their corresponding attack types.

A screenshot of a computer

Description automatically generated