# CYBER SPIES

## CyberSecurity Threat Intelligence Platform Management System

Database Design - Phase 1 Documentation

### Group Information

**Group Name:** Cyber Spies
**Course:** Database Management Systems (DBMS)
**Project:** CyberSecurity Threat Intelligence Platform Management System

**Group Members:**

| | | |
|---|---|---|
| 1. | Muhammad Umair Amjad | 24L-0711 |
| 2. | Hashir Ahmad | 24L-0729 |
| 3. | Muhammad Ali Lodhi | 24L-0703 |

# 1. List of Tables

The CTI database consists of 13 tables: 9 core tables and 4 junction (bridge) tables for many-to-many relationships.

| # | Table Name | Purpose |
|---|---|---|
| 1 | ThreatActors | Stores known threat actors (APT groups, individuals) |
| 2 | ThreatFeeds | External intelligence feeds providing IOC data |
| 3 | Indicators (IOCs) | Indicators of Compromise: IP, Domain, Hash, URL |
| 4 | TTPs | MITRE ATT&CK tactics, techniques & procedures |
| 5 | Campaigns | Attack campaigns attributed to threat actors |
| 6 | Users | System users with roles: Admin, Analyst, Manager |
| 7 | Vulnerabilities | CVE-tracked software vulnerabilities |
| 8 | Incidents | Detected security incidents linked to campaigns |
| 9 | Reports | Analyst reports tied to incidents (TLP classified) |
| J1 | Actor_TTP | Junction: ThreatActors <-> TTPs (M:M) |
| J2 | Campaign_IOC | Junction: Campaigns <-> Indicators (M:M) |
| J3 | Incident_IOC | Junction: Incidents <-> Indicators (M:M) |
| J4 | Incident_Vulnerability | Junction: Incidents <-> Vulnerabilities (M:M) |

# 2. Table Definitions with Attributes

## ThreatActors

*Relationship: Independent entity - no FK dependencies*

| Column | Data Type | NOT NULL | Default | Constraint / Notes |
|---|---|---|---|---|
| actor_id | `INT` | YES | IDENTITY | *Primary Key - auto increment* |
| name | `NVARCHAR(255)` | YES | | *UNIQUE - actor name required* |
| alias | `NVARCHAR(255)` | | | *Known alias or nickname* |
| group_name | `NVARCHAR(255)` | | | *APT or threat group name* |
| motivation | `NVARCHAR(255)` | | | *e.g. Financial, Espionage, Hacktivism* |
| country | `NVARCHAR(100)` | | | *Origin/attributed country* |
| first_seen | `DATE` | | | *Date first observed* |
| last_seen | `DATE` | | | *CHECK: last_seen >= first_seen* |
| risk_level | `NVARCHAR(50)` | | | *CHECK: Critical / High / Medium / Low* |
| description | `NVARCHAR(MAX)` | | | *Detailed actor profile* |
| created_at | `DATETIME` | YES | GETDATE() | *Auto-set on insert* |

## ThreatFeeds

*Relationship: Independent entity - no FK dependencies*

| Column | Data Type | NOT NULL | Default | Constraint / Notes |
|---|---|---|---|---|
| feed_id | `INT` | YES | IDENTITY | *Primary Key* |
| name | `NVARCHAR(255)` | YES | | *UNIQUE feed name* |
| provider | `NVARCHAR(255)` | YES | | *Provider organization - required* |
| api_url | `NVARCHAR(500)` | | | *REST API endpoint URL* |
| update_frequency | `NVARCHAR(100)` | | | *e.g. Hourly, Daily, Weekly* |
| format | `NVARCHAR(100)` | | | *CHECK: STIX/JSON/XML/CSV/MISP/Other* |
| reliability_score | `DECIMAL(3,2)` | | 0.50 | *CHECK: 0.00 to 1.00* |
| last_updated | `DATETIME` | | | *Timestamp of last sync* |

## Indicators (IOCs)

*Relationship: ThreatFeeds (1) -> (M) Indicators*

| Column | Data Type | NOT NULL | Default | Constraint / Notes |
|---|---|---|---|---|
| ioc_id | `INT` | YES | IDENTITY | *Primary Key* |
| type | `NVARCHAR(50)` | YES | | *CHECK: IP/Domain/Hash/URL/Email/Filename* |
| value | `NVARCHAR(500)` | YES | | *The actual IOC value - UNIQUE per type* |
| confidence_score | `DECIMAL(3,2)` | | 0.50 | *CHECK: 0.00 to 1.00* |
| first_seen | `DATETIME` | | | *First observation timestamp* |
| last_seen | `DATETIME` | | | *CHECK: last_seen >= first_seen* |
| is_active | `BIT` | YES | 1 | *1=Active / 0=Retired* |
| feed_id | `INT` | | | *FK -> ThreatFeeds.feed_id (SET NULL)* |

## TTPs

*Relationship: Independent entity - no FK dependencies*

| Column | Data Type | NOT NULL | Default | Constraint / Notes |
|---|---|---|---|---|
| ttp_id | `INT` | YES | IDENTITY | *Primary Key* |
| name | `NVARCHAR(255)` | YES | | *TTP display name* |
| mitre_attack_id | `NVARCHAR(50)` | | | *UNIQUE - e.g. T1059.001* |
| tactic | `NVARCHAR(255)` | YES | | *MITRE tactic - required* |
| technique | `NVARCHAR(255)` | YES | | *MITRE technique - required* |
| sub_technique | `NVARCHAR(255)` | | | *Optional sub-technique* |
| severity | `NVARCHAR(50)` | YES | | *CHECK: Critical/High/Medium/Low* |
| description | `NVARCHAR(MAX)` | | | *Detailed description* |

## Campaigns

*Relationship: ThreatActors (1) -> (M) Campaigns*

| Column | Data Type | NOT NULL | Default | Constraint / Notes |
|---|---|---|---|---|
| campaign_id | `INT` | YES | IDENTITY | *Primary Key* |
| name | `NVARCHAR(255)` | YES | | *UNIQUE campaign name* |
| start_date | `DATE` | | | *Campaign start date* |

| | | | | |
|---|---|---|---|---|
| end_date | `DATE` | | | *CHECK: end_date >= start_date* |
| objective | `NVARCHAR(MAX)` | | | *Campaign goal / objective* |
| status | `NVARCHAR(100)` | YES | 'Active' | *CHECK: Active/Inactive/Closed/Under Investigation* |
| actor_id | `INT` | | | *FK -> ThreatActors.actor_id (SET NULL)* |

## Users

*Relationship: Independent entity - no FK dependencies*

| Column | Data Type | NOT NULL | Default | Constraint / Notes |
|---|---|---|---|---|
| user_id | `INT` | YES | IDENTITY | *Primary Key* |
| username | `NVARCHAR(100)` | YES | | *UNIQUE username* |
| password_hash | `NVARCHAR(255)` | YES | | *Stored as bcrypt hash* |
| email | `NVARCHAR(255)` | YES | | *UNIQUE - CHECK email format* |
| role | `NVARCHAR(50)` | YES | | *CHECK: Admin / Analyst / Manager* |
| created_at | `DATETIME` | YES | GETDATE() | *Auto-set on account creation* |
| last_login | `DATETIME` | | | *Updated on each login* |
| is_active | `BIT` | YES | 1 | *1=Active / 0=Deactivated* |

## Vulnerabilities

*Relationship: Independent entity - no FK dependencies*

| Column | Data Type | NOT NULL | Default | Constraint / Notes |
|---|---|---|---|---|
| vuln_id | `INT` | YES | IDENTITY | *Primary Key* |
| cve_id | `NVARCHAR(50)` | | | *UNIQUE - e.g. CVE-2024-1234* |
| description | `NVARCHAR(MAX)` | YES | | *Vulnerability description - required* |
| cvss_score | `DECIMAL(4,2)` | | | *CHECK: 0.0 to 10.0* |
| published_date | `DATE` | | | *NVD publish date* |
| patch_available | `BIT` | YES | 0 | *0=No patch yet / 1=Patched* |
| affected_products | `NVARCHAR(MAX)` | | | *Comma-separated product list* |
| exploit_available | `BIT` | YES | 0 | *0=No PoC / 1=Exploit in wild* |

## Incidents

*Relationship: Campaign (1)->(M) Incidents | User (1)->(M) Incidents*

| Column | Data Type | NOT NULL | Default | Constraint / Notes |
|---|---|---|---|---|
| incident_id | `INT` | YES | IDENTITY | *Primary Key* |
| title | `NVARCHAR(255)` | YES | | *Incident title - required* |
| description | `NVARCHAR(MAX)` | | | *Detailed incident description* |
| date_detected | `DATETIME` | YES | | *CHECK: date_detected <= GETDATE()* |
| severity | `NVARCHAR(50)` | YES | | *CHECK: Critical/High/Medium/Low* |
| status | `NVARCHAR(100)` | YES | 'Open' | *CHECK: Open/Investigating/Contained/Resolved/Closed* |
| affected_systems | `NVARCHAR(MAX)` | | | *List of impacted systems* |
| campaign_id | `INT` | | | *FK -> Campaigns.campaign_id (SET NULL)* |
| reported_by | `INT` | | | *FK -> Users.user_id (SET NULL)* |

## Reports

*Relationship: Incident (1)->(M) Reports | User (1)->(M) Reports*

| Column | Data Type | NOT NULL | Default | Constraint / Notes |
|---|---|---|---|---|
| report_id | `INT` | YES | IDENTITY | *Primary Key* |
| title | `NVARCHAR(255)` | YES | | *Report title - required* |
| summary | `NVARCHAR(MAX)` | | | *Executive summary* |
| classification | `NVARCHAR(50)` | YES | | *CHECK: TLP Red/Amber/Green/White* |
| created_at | `DATETIME` | YES | GETDATE() | *Auto-set* |
| author_id | `INT` | | | *FK -> Users.user_id (SET NULL)* |
| incident_id | `INT` | | | *FK -> Incidents.incident_id (SET NULL)* |

## Junction Tables (Many-to-Many)

## Actor_TTP

| Column | Data Type | NOT NULL | Default | Constraint / Notes |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| actor_id | `INT` | YES | | *PK + FK -> ThreatActors.actor_id (ON DELETE CASCADE)* |
| ttp_id | `INT` | YES | | *PK + FK -> TTPs.ttp_id (ON DELETE CASCADE)* |
| (actor_id, ttp_id) | — | — | | *Composite Primary Key* |

## Campaign_IOC

| Column | Data Type | NOT NULL | Default | Constraint / Notes |
|---|---|---|---|---|
| campaign_id | `INT` | YES | | *PK + FK -> Campaigns.campaign_id (ON DELETE CASCADE)* |
| ioc_id | `INT` | YES | | *PK + FK -> Indicators.ioc_id (ON DELETE CASCADE)* |
| (campaign_id, ioc_id) | — | — | | *Composite Primary Key* |

## Incident_IOC

| Column | Data Type | NOT NULL | Default | Constraint / Notes |
|---|---|---|---|---|
| incident_id | `INT` | YES | | *PK + FK -> Incidents.incident_id (ON DELETE CASCADE)* |
| ioc_id | `INT` | YES | | *PK + FK -> Indicators.ioc_id (ON DELETE CASCADE)* |
| (incident_id, ioc_id) | — | — | | *Composite Primary Key* |

## Incident_Vulnerability

| Column | Data Type | NOT NULL | Default | Constraint / Notes |
|---|---|---|---|---|
| incident_id | `INT` | YES | | *PK + FK -> Incidents.incident_id (ON DELETE CASCADE)* |
| vuln_id | `INT` | YES | | *PK + FK -> Vulnerabilities.vuln_id (ON DELETE CASCADE)* |
| (incident_id, vuln_id) | — | — | | *Composite Primary Key* |

# 3. Relationships Summary

| Relationship | Type | Implementation |
|---|---|---|
| ThreatActors -> Campaigns | 1 : M | FK actor_id in Campaigns (SET NULL on delete) |
| ThreatFeeds -> Indicators | 1 : M | FK feed_id in Indicators (SET NULL on delete) |
| Campaigns -> Incidents | 1 : M | FK campaign_id in Incidents (SET NULL) |
| Users -> Incidents | 1 : M | FK reported_by in Incidents (SET NULL) |
| Users -> Reports | 1 : M | FK author_id in Reports (SET NULL) |
| Incidents -> Reports | 1 : M | FK incident_id in Reports (SET NULL) |
| ThreatActors <-> TTPs | M : M | Bridge: Actor_TTP (CASCADE delete) |
| Campaigns <-> Indicators | M : M | Bridge: Campaign_IOC (CASCADE delete) |
| Incidents <-> Indicators | M : M | Bridge: Incident_IOC (CASCADE delete) |
| Incidents <-> Vulnerabilities | M : M | Bridge: Incident_Vulnerability (CASCADE) |