**📌 Requirements Recap:**

* Domain: ✅ Cyber Security
* Entities: ✅ 10 entities (minimum)
* Attributes per entity: ✅ At least 10 with data types & justification
* Relationships: ✅ 1:1, 1:N, M:N
* Keys: ✅ Primary & Foreign Keys
* Participation: ✅ Total & Partial
* Others: ✅ Include weak/strong entities

**🔐 Domain: Cyber Security — Malware Analysis & Threat Management System**

**✅ Entities and Attributes**

**1. Malware**

| **Attribute** | **Data Type** | **Justification** |
| --- | --- | --- |
| MalwareID | Integer (PK) | Unique identifier |
| MalwareName | String | Descriptive name |
| Type | String | E.g., ransomware, worm |
| FirstDetectedDate | DateTime | Date malware first detected |
| Hash\_MD5 | String | MD5 hash of file |
| Hash\_SHA256 | String | Secure SHA256 hash |
| SeverityLevel | String | High/Medium/Low |
| Aliases | String[] (Multivalued) | Known by multiple names |
| DetectedByAnalystID | Integer (FK) | Linked to Analyst entity |
| PlatformTargeted | String | OS/Platform affected |

**2. Signature**

| **Attribute** | **Data Type** | **Justification** |
| --- | --- | --- |
| SignatureID | Integer (PK) | Unique ID |
| MalwareID | Integer (FK) | Related malware |
| Pattern | String | Unique pattern |
| DetectionMethod | String | Static/Dynamic |
| CreationDate | DateTime | When signature was added |
| LastUpdated | DateTime | Timestamp of last update |
| IsActive | Boolean | Whether still in use |
| SignatureType | String | E.g., file, behavior |
| ToolUsed | String | Tool used to create it |
| ConfidenceScore | Float | Accuracy % |

**3. Analyst**

| **Attribute** | **Data Type** | **Justification** |
| --- | --- | --- |
| AnalystID | Integer (PK) | Unique analyst ID |
| Name | String | Full name |
| Email | String | Contact email |
| PhoneNumber | String | For alerts/calls |
| ExperienceYears | Integer | Experience in years |
| Specialization | String | E.g., forensics, malware |
| Organization | String | Company name |
| CertificationList | String[] (Multivalued) | OSCP, CEH, etc. |
| AnalystLevel | String | Junior/Senior |
| DateJoined | DateTime | Hiring date |

**4. Behavior**

| **Attribute** | **Data Type** | **Justification** |
| --- | --- | --- |
| BehaviorID | Integer (PK) | Unique behavior ID |
| Description | Text | What the behavior does |
| IsStealthy | Boolean | Whether it evades detection |
| NetworkUsage | Boolean | If it affects network |
| RegistryChange | Boolean | If it modifies registry |
| FileDrop | Boolean | If it drops payloads |
| PersistenceMethod | String | How it stays active |
| PrivilegeEscalation | Boolean | If it elevates privilege |
| MalwareID | Integer (FK) | Associated malware |
| TimestampDetected | DateTime | When behavior was seen |

**5. Device**

| **Attribute** | **Data Type** | **Justification** |
| --- | --- | --- |
| DeviceID | Integer (PK) | Unique device ID |
| Hostname | String | Machine name |
| IPAddress | String | IP for tracking |
| MACAddress | String | Unique network ID |
| Location | String | Physical site |
| OS | String | Windows/Linux etc. |
| Owner | String | Who owns the device |
| IsCriticalSystem | Boolean | Critical asset flag |
| Status | String | Online/Offline/Infected |
| LastScanDate | DateTime | Date of last scan |

**6. InfectionReport *(Weak Entity)***

| **Attribute** | **Data Type** | **Justification** |
| --- | --- | --- |
| ReportNumber | Integer (Partial Key) | Not unique without DeviceID |
| DeviceID | Integer (FK) | Weak on Device |
| MalwareID | Integer (FK) | Malware involved |
| DateReported | DateTime | Timestamp |
| InfectionSeverity | String | Critical/Low |
| ActionTaken | String | Quarantined/Deleted |
| ReportStatus | String | Open/Closed |
| Description | Text | Full details |
| FilePath | String | File involved |
| AnalystID | Integer (FK) | Who analyzed it |

**7. Platform**

| **Attribute** | **Data Type** | **Justification** |
| --- | --- | --- |
| PlatformID | Integer (PK) | Unique ID |
| Name | String | E.g., Windows |
| Version | String | E.g., 10.0.19044 |
| Architecture | String | x86/x64/ARM |
| Vendor | String | Microsoft, Linux |
| PatchLevel | String | Latest patch version |
| Supported | Boolean | Still supported or deprecated |
| ThreatLevel | String | Risk Level |
| IsMobile | Boolean | If it's a mobile OS |
| Notes | Text | Comments/notes |

**8. ThreatIntelFeed**

| **Attribute** | **Data Type** | **Justification** |
| --- | --- | --- |
| FeedID | Integer (PK) | Unique feed ID |
| FeedName | String | Source name |
| URL | String | API or endpoint |
| SourceType | String | OSINT, Commercial |
| UpdateFrequency | String | Daily, Hourly |
| LastFetched | DateTime | Last fetch timestamp |
| ConfidenceLevel | Float | Trust score |
| Description | Text | Feed details |
| Format | String | JSON, STIX, etc. |
| AnalystID | Integer (FK) | Who subscribed it |

**9. Incident**

| **Attribute** | **Data Type** | **Justification** |
| --- | --- | --- |
| IncidentID | Integer (PK) | Unique identifier |
| Title | String | Summary |
| Description | Text | Full narrative |
| Severity | String | High, Medium, Low |
| AffectedDeviceID | Integer (FK) | Target device |
| MalwareInvolvedID | Integer (FK) | Optional |
| DateOccurred | DateTime | When it happened |
| IsResolved | Boolean | Current status |
| AnalystID | Integer (FK) | Who is assigned |
| ResponseTimeHours | Float | Resolution metric |

**10. FirewallLog**

| **Attribute** | **Data Type** | **Justification** |
| --- | --- | --- |
| LogID | Integer (PK) | Unique log ID |
| DeviceID | Integer (FK) | Source machine |
| Timestamp | DateTime | When it happened |
| SourceIP | String | Who sent the packet |
| DestinationIP | String | Who received it |
| Port | Integer | Port number |
| Protocol | String | TCP, UDP |
| Action | String | Allowed/Blocked |
| MalwareID (optional) | Integer (FK) | Match with known malware? |
| Severity | String | Informational/Critical |

**🔗 Relationship Overview**

| **Relationship** | **Type** | **Participation** |
| --- | --- | --- |
| Malware ↔ Signature | 1:N | Total from Signature |
| Malware ↔ Behavior | 1:N | Partial from both |
| Malware ↔ Analyst (via Analysis) | M:N | Total from Malware |
| Malware ↔ Platform | M:N | Partial |
| Device → InfectionReport | 1:N | Weak relationship, total from report |
| Malware → InfectionReport | 1:N | Total from report |
| Analyst → ThreatIntelFeed | 1:N | Partial |
| Device ↔ FirewallLog | 1:N | Total from log |
| Malware ↔ Incident | 1:N | Partial |
| Device ↔ Incident | 1:N | Total from incident |

**📄 Final Submission Content (What I’ll Prepare)**

1. **Entities + Attributes + Data Types** with justification → in a **tabular format**
2. **ER Diagram** with:
   * Primary & foreign keys
   * Weak & strong entities
   * Relationship types (1:1, 1:N, M:N)
   * Total and partial participation
   * Multivalued attributes
   * Derived attributes (if needed)