Documentação do Esquema de Banco de Dados: silver.microsoft_security_incident

1 Arquivo DDL Original: security_ddl.sql

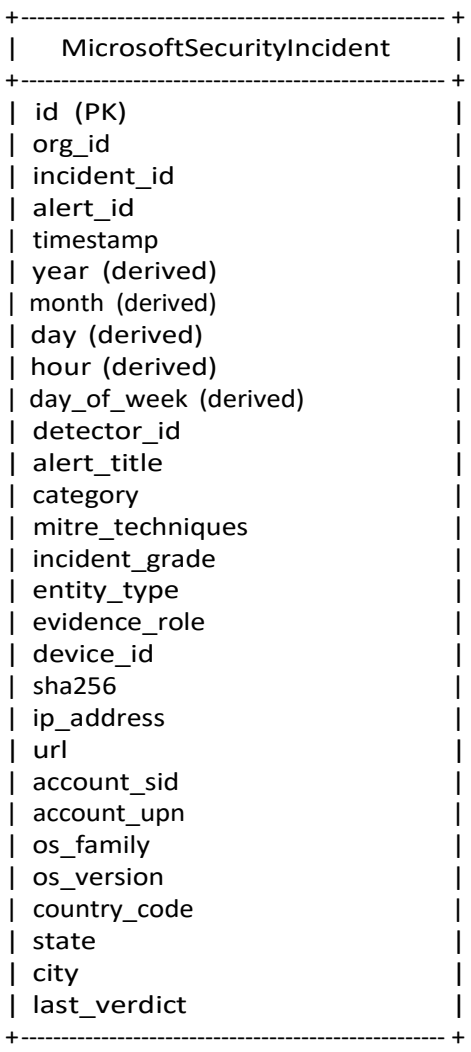
```
CREATE SCHEMA IF NOT EXISTS silver;
DROP TABLE IF EXISTS silver.microsoft_security_incident;
CREATE TABLE silver.microsoft_security_incident (
    -- Identificadores
    id BIGINT PRIMARY KEY,
    org_id INT NOT NULL,
    incident_id INT NOT NULL,
    alert_id INT NOT NULL,
    timestamp TIMESTAMP NOT NULL,
    year INT GENERATED ALWAYS AS (EXTRACT(YEAR FROM timestamp)::INT) STORED,
    month INT GENERATED ALWAYS AS (EXTRACT(MONTH FROM timestamp)::INT) STORED,
    day INT GENERATED ALWAYS AS (EXTRACT(DAY FROM timestamp)::INT) STORED,
    hour INT GENERATED ALWAYS AS (EXTRACT(HOUR FROM timestamp)::INT) STORED,
    day_of_week INT GENERATED ALWAYS AS (EXTRACT(DOW FROM timestamp)::INT) STORED,
    detector_id INT NOT NULL,
    alert_title INT NOT NULL,
    category INT NOT NULL,
    mitre_techniques INT NOT NULL,
    incident_grade INT NOT NULL,
    entity_type INT NOT NULL,
    evidence_role INT NOT NULL,
    device_id BIGINT,
    sha256 BIGINT,
    ip_address BIGINT,
    url BIGINT,
    account_sid BIGINT,
    account_upn BIGINT,
    os_family INT NOT NULL,
    os_version INT NOT NULL,
    country_code INT NOT NULL,
    state INT NOT NULL,
    city INT NOT NULL,
    last_verdict INT NOT NULL
);
```

2 Modelo Entidade-Relacionamento (MER)

O Modelo Entidade-Relacionamento (MER) representa o modelo conceitual dos dados, focando em entidades, atributos e relacionamentos. **Entidade**: MicrosoftSecurityIncident (representa um incidente de segurança da Microsoft).

- **Atributos**:
  - id: BIGINT (chave primária, identificador único do registro).
  - org_id: INT (identificador da organização, obrigatório).
  - incident_id: INT (identificador do incidente, obrigatório).
  - alert_id: INT (identificador do alerta, obrigatório).
  - timestamp: TIMESTAMP (data e hora do incidente, obrigatório; base para atributos derivados).
  - year: INT (ano extraído do timestamp, gerado automaticamente).
  - month: INT (mês extraído do timestamp, gerado automaticamente).
  - day: INT (dia extraído do timestamp, gerado automaticamente).
  - hour: INT (hora extraída do timestamp, gerado automaticamente).
  - day_of_week: INT (dia da semana extraído do timestamp, gerado automaticamente).
  - detector_id: INT (identificador do detector, obrigatório).
  - alert_title: INT (título do alerta, obrigatório; possivelmente um código numérico).
  - category: INT (categoria do incidente, obrigatório; possivelmente um código).
  - mitre_techniques: INT (técnicas MITRE associadas, obrigatório; possivelmente um código).
  - incident_grade: INT (grau do incidente, obrigatório; possivelmente um código).
  - entity_type: INT (tipo de entidade envolvida, obrigatório; possivelmente um código).
  - evidence_role: INT (papel da evidência, obrigatório; possivelmente um código).
  - device_id: BIGINT (identificador do dispositivo, opcional).
  - sha256: BIGINT (hash SHA-256, opcional; possivelmente relacionado a arquivos ou evidências).
  - ip_address: BIGINT (endereço IP, opcional; possivelmente codificado como inteiro).
  - url: BIGINT (URL associada, opcional; possivelmente codificada).
  - account_sid: BIGINT (SID da conta, opcional).
  - account_upn: BIGINT (UPN da conta, opcional).
  - os_family: INT (família do sistema operacional, obrigatório; possivelmente um código).
  - os_version: INT (versão do sistema operacional, obrigatório; possivelmente um código).
  - country_code: INT (código do país, obrigatório; possivelmente um código ISO).
  - state: INT (estado/região, obrigatório; possivelmente um código).
  - city: INT (cidade, obrigatório; possivelmente um código).
  - last_verdict: INT (veredicto final, obrigatório; possivelmente um código).
- **Observações**: Atributos como year, month etc. são derivados (calculated fields) e não são editáveis manualmente. Muitos atributos parecem ser códigos ou IDs que poderiam referenciar dimensões externas em um modelo mais completo, mas aqui estão denormalizados.

3 Diagrama Entidade-Relacionamento (DER)



- **Legenda**:
  - PK: Chave Primária.
  - (derived): Atributo gerado automaticamente a partir de timestamp.

4 Diagrama Lógico de Dados (DLD)

Schema: silver

Tabela: microsoft_security_incident

Coluna	Tipo	Nullable?	Observações
id	BIGINT	Não	PRIMARY KEY
org_id	INT	Não	
incident_id	INT	Não	
alert_id	INT	Não	
timestamp	TIMESTAMP	Não	
year	INT	Não	GENERATED ALWAYS AS (EXTRACT(YEAR FROM timestamp)::INT
month	INT	Não	GENERATED ALWAYS AS (EXTRACT(MONTH FROM timestamp)::IN
day	INT	Não	GENERATED ALWAYS AS (EXTRACT(DAY FROM timestamp)::INT)
hour	INT	Não	GENERATED ALWAYS AS (EXTRACT(HOUR FROM timestamp)::INT
day_of_week	INT	Não	GENERATED ALWAYS AS (EXTRACT(DOW FROM timestamp)::INT)
detector_id	INT	Não	
alert_title	INT	Não	
category	INT	Não	
mitre_techniques	INT	Não	
incident_grade	INT	Não	
entity_type	INT	Não	
evidence_role	INT	Não	
device_id	BIGINT	Sim	
sha256	BIGINT	Sim	
ip_address	BIGINT	Sim	
url	BIGINT	Sim	
account_sid	BIGINT	Sim	
account_upn	BIGINT	Sim	
os_family	INT	Não	
os_version	INT	Não	
country_code	INT	Não	
state	INT	Não	
city	INT	Não	
last_verdict	INT	Não	