silver.microsoft_security_incident

1 Resumo e Observações

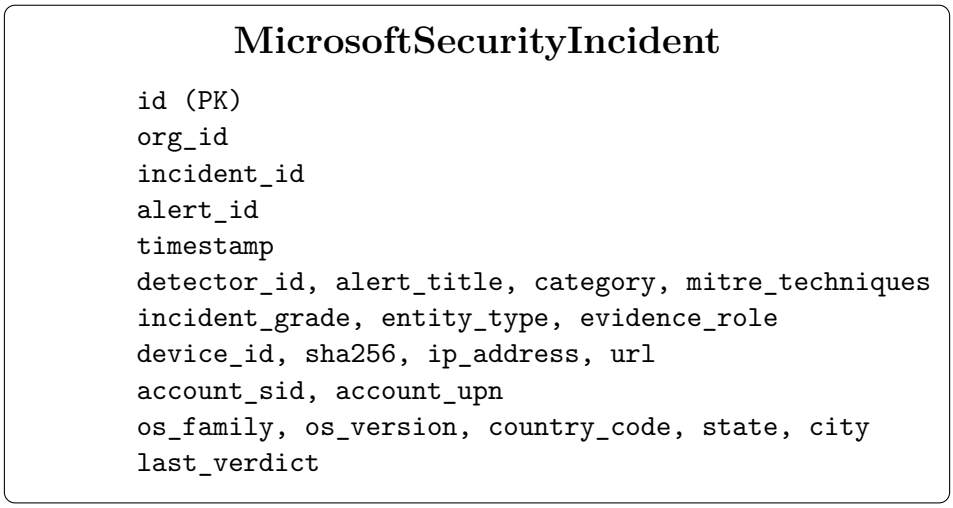
Este documento contém:

- O DDL original para referência.
- Um diagrama MER.
- Um DLD

2 DDL (referência)

```sql
CREATE SCHEMA IF NOT EXISTS silver;
DROP TABLE IF EXISTS silver.microsoft_security_incident;
CREATE TABLE silver.microsoft_security_incident (
  -- Identificadores
  id  INT PRIMARY KEY,
  org_id INT NOT NULL,
  incident_id INT NOT NULL,
  alert_id INT NOT NULL,
  timestamp TIMESTAMP NOT NULL,
  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  INT,
  sha256  INT,
  ip_address  INT,
  url  INT,
  account_sid  INT,
  account_upn  INT,
  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
);
```

3 Modelo Entidade-Relacionamento (MER)



4 Diagrama Lógico de Dados (DLD) — Tabela de Colunas

Tabela 1: **Tabela:** `silver.microsoft_security_incident`

Coluna	Tipo	Null	Observações
id	INT	Não	PRIMARY KEY — identificador único.
org_id	INT	Não	Identificador da organização.
incident_id	INT	Não	Identificador do incidente.
alert_id	INT	Não	Identificador do alerta.
timestamp	TIMESTAMP	Não	Data e hora do incidente.
detector_id	INT	Não	ID do detector que gerou o alerta.
alert_title	INT	Não	Código/título do alerta.
category	INT	Não	Categoria do incidente.
mitre_techniques	INT	Não	Técnicas MITRE associadas.
incident_grade	INT	Não	Grau/criticidade do incidente.
entity_type	INT	Não	Tipo de entidade envolvida.
evidence_role	INT	Não	Papel da evidência.
device_id	INT	Sim	Identificador do dispositivo.
sha256	INT	Sim	Hash SHA-256.
ip_address	INT	Sim	Endereço IP armazenado como inteiro.
url	INT	Sim	URL codificada.
account_sid	INT	Sim	SID da conta.
account_upn	INT	Sim	UPN da conta.
os_family	INT	Não	Família do sistema operacional.
os_version	INT	Não	Versão do SO.
country_code	INT	Não	Código do país.
state	INT	Não	Estado/região.

(continua na próxima página)

Continuação da tabela ...

Coluna	Tipo	Null	Observações
city	INT	Não	Cidade.
last_verdict	INT	Não	Veredicto final.