silver.microsoft_security_incident

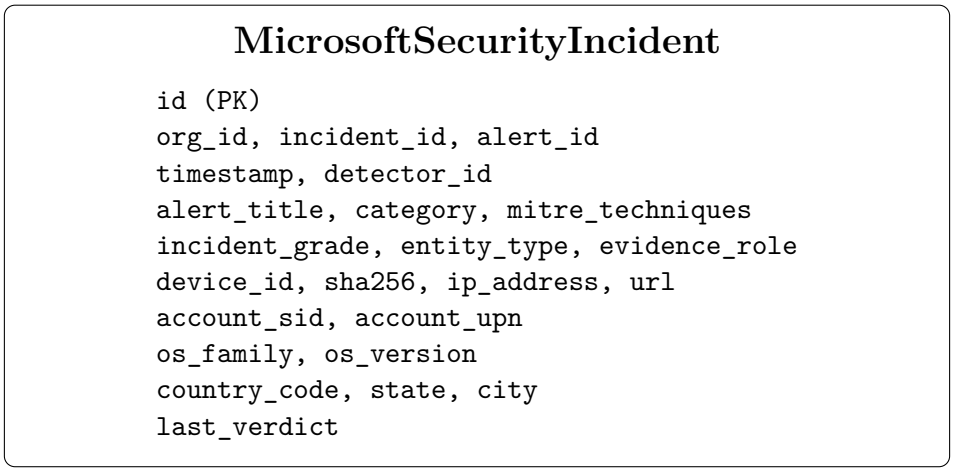
1 Resumo e Observações

Este documento contém:

- O DDL.
- Um DLD.

```sql
CREATE SCHEMA IF NOT EXISTS silver;
DROP TABLE IF EXISTS silver.microsoft_security_incident;
CREATE TABLE silver.microsoft_security_incident (
  id BIGINT 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,s
  alert_title VARCHAR(500) NOT NULL,
  category VARCHAR(100) NOT NULL,
  mitre_techniques VARCHAR(200) NOT NULL,
  incident_grade INT NOT NULL,
  entity_type INT NOT NULL,
  evidence_role INT NOT NULL,
  device_id BIGINT,
  sha256 CHAR(64),
  ip_address INET,
  url TEXT,
  account_sid VARCHAR(200),
  account_upn VARCHAR(255),
  os_family VARCHAR(50) NOT NULL,
  os_version VARCHAR(50) NOT NULL,
  country_code CHAR(2) NOT NULL,
  state VARCHAR(100) NOT NULL,
  city VARCHAR(100) NOT NULL,
  last_verdict VARCHAR(50) NOT NULL
);
```

2 Modelo Entidade-Relacionamento (MER)



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

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

Coluna	Tipo	Null	Observações
id	BIGINT	Não	PRIMARY KEY — identificador único da linha.
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/alerta.
detector_id	INT	Não	ID do detector que gerou o alerta.
alert_title	VARCHAR(500)	Não	Título/descrição do alerta.
category	VARCHAR(100)	Não	Categoria do incidente.
mitre_techniques	VARCHAR(200)	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 no incidente.
device_id	BIGINT	Sim	Identificador do dispositivo afetado.
sha256	CHAR(64)	Sim	Hash SHA-256 em hexadecimal.
ip_address	INET	Sim	Endereço IP (IPv4 ou IPv6).
url	TEXT	Sim	URL maliciosa ou de origem do ataque.
account_sid	VARCHAR(200)	Sim	SID da conta Windows.
account_upn	VARCHAR(255)	Sim	User Principal.
os_family	VARCHAR(50)	Não	Família do SO.
os_version	VARCHAR(50)	Não	Versão específica do SO.
country_code	CHAR(2)	Não	Código ISO 3166-1 alfa-2 (BR, US, FR, etc.).
state	VARCHAR(100)	Não	Estado ou região (São Paulo, California, etc.).
city	VARCHAR(100)	Não	Cidade de origem do incidente.
last_verdict	VARCHAR(50)	Não	Veredicto final (Malicious, Suspicious, Clean, etc.).

MICROSOFT_SECURITY_INCIDENT		
PK	id	Bigint
NOT_NULL	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	Varchar(500)
NOT_NULL	category	Varchar(100)
NOT_NULL	mitre_techniques	Varchar(200)
NOT_NULL	incident_grade	Int
NOT_NULL	entity_type	Int
NOT_NULL	evidence_role	Int
	device_id	Bigint
	sha256	Char(64)
	ip_address	Inet
	url	Text
	account_sid	Varchar(200)
	account_upn	Varchar(255)
	os_family	Varchar(50)
	os_version	Varchar(50)
	country_code	Char(2)
	state	Varchar(100)
	city	Varchar(100)
	last_verdict	Varchar(50)