

Dicionario de Dados - Camada Silver

Fonte do DDL: security_ddl.sql. Dataset de origem: Microsoft Security Incident Prediction (Kaggle). O dicionario abaixo descreve os campos persistidos na camada silver apos padronizacoes e codificacoes.

id (BIGINT) - NOT NULL PRIMARY KEY

org_id (INT) - NOT NULL

incident_id (INT) - NOT NULL

alert_id (INT) - NOT NULL

timestamp (TIMESTAMP) - NOT NULL

year (INT) - GENERATED NOT NULL

month (INT) - GENERATED NOT NULL

day (INT) - GENERATED NOT NULL

hour (INT) - GENERATED NOT NULL

day_of_week (INT) - GENERATED 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 (BIGINT) - NULLABLE

sha256 (BIGINT) - NULLABLE

ip_address (BIGINT) - NULLABLE

url (BIGINT) - NULLABLE

account_sid (BIGINT) - NULLABLE

account_upn (BIGINT) - NULLABLE

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

Mapeamentos chave:

Referencias: Kaggle - Microsoft Security Incident Prediction
(<https://www.kaggle.com/datasets/microsoft/microsoft-security-incident-prediction/data>). Consulta em
07/11/2025.