

Dicionario de Dados - Camada Silver

Table

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

Identificador

org_id (INT) - NOT NULL

Identificador

incident_id (INT) - NOT NULL

Agrupador

alert_id (INT) - NOT NULL

Identificador

timestamp (TIMESTAMP) - NOT NULL

Data

year (INT) - GENERATED NOT NULL

Ano

month (INT) - GENERATED NOT NULL

Mes

day (INT) - GENERATED NOT NULL

Dia

hour (INT) - GENERATED NOT NULL

Hora

day_of_week (INT) - GENERATED NOT NULL

Dia da Semana

detector_id (INT) - NOT NULL

Codificador

alert_title (INT) - NOT NULL

Titulo

category (INT) - NOT NULL

Categoria

mitre_techniques (INT) - NOT NULL

Codificador

incident_grade (INT) - NOT NULL

Classificacao

entity_type (INT) - NOT NULL

Tipo

evidence_role (INT) - NOT NULL

Papel

device_id (BIGINT) - NULLABLE

sha256 (BIGINT) - NULLABLE	Identificação
ip_address (BIGINT) - NULLABLE	Hash IP
url (BIGINT) - NULLABLE	Endereço de URL
account_sid (BIGINT) - NULLABLE	SID da conta
account_upn (BIGINT) - NULLABLE	UPN/Email
os_family (INT) - NOT NULL	Família do sistema operacional
os_version (INT) - NOT NULL	Versão do sistema operacional
country_code (INT) - NOT NULL	País
state (INT) - NOT NULL	Estado
city (INT) - NOT NULL	Cidade
last_verdict (INT) - NOT NULL	Último veredito
Mapeamentos chave:	- incide

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