Dicionário de dados

Coluna	Tipo	Descrição
Id	integer	ID único para cada par OrgId-IncidentId
OrgId	integer	Identificador da organização
IncidentId	integer	Identificador único do incidente na organização
AlertId	integer	Identificador único de um alerta
Timestamp	varchar(30)	Momento em que o alerta foi criado
DetectorId	integer	ID único do detector que gerou o alerta
AlertTitle	integer	Título do alerta
Category	varchar(30)	Categoria do alerta
MitreTechniques	varchar(100)	Técnicas MITRE ATT&CK envolvidas no alerta
IncidentGrade	varchar(20)	Grau atribuído ao incidente pelo SOC
ActionGrouped	integer	Ação de remediação do alerta pelo SOC (nível alto)
ActionGranular	integer	Ação de remediação do alerta pelo SOC (nível detalhado)
EntityType	varchar(40)	Tipo de entidade envolvida no alerta
EvidenceRole	enum	Papel da evidência na investigação ('Related', 'Impacted')
DeviceId	integer	Identificador único do dispositivo
Sha256	integer	Hash SHA-256 do arquivo
IpAddress	integer	Endereço IP envolvido
Url	integer	URL envolvida
AccountSid	integer	Identificador da conta local
AccountUpn	integer	Identificador da conta de e-mail
AccountObjectId	integer	Identificador da conta Entra ID
AccountName	integer	Nome da conta local
DeviceName	integer	Nome do dispositivo
NetworkMessageId	integer	Identificador da mensagem de e-mail no nível da organização
EmailClusterId	integer	Identificador único do agrupamento de e-mails

Coluna	Tipo	Descrição
RegistryKey	integer	Chave de registro envolvida
RegistryValueName	integer	Nome do valor de registro
RegistryValueData	integer	Dados do valor de registro
ApplicationId	integer	Identificador único da aplicação
ApplicationName	integer	Nome da aplicação
OAuthApplicationId	integer	Identificador da aplicação OAuth
ThreatFamily	varchar(100)	Família de malware associada ao arquivo
FileName	integer	Nome do arquivo
FolderPath	integer	Caminho da pasta do arquivo
ResourceIdName	integer	Nome do recurso do Azure
ResourceType	varchar(100)	Tipo de recurso do Azure
Roles	varchar(20)	Metadados adicionais sobre o papel da evidência no alerta
OSFamily	integer	Família do sistema operacional
OSVersion	integer	Versão do sistema operacional
AntispamDirection	varchar(100)	Direção do filtro antispam
SuspicionLevel	enum	Nível de suspeita ('Suspicious', 'Incriminated')
LastVerdict	varchar(100)	Veredito final da análise de ameaça
CountryCode	integer	Código do país onde a evidência aparece
State	integer	Estado onde a evidência aparece
City	integer	Cidade onde a evidência aparece