# Habilitando o workflow avançado de Incidente declarado

Para usar o workflow avançado de Incidente declarado, você deve configurar a ferramenta SIEM para enviar dados ao Archer usando APIs. A tabela a seguir inclui os campos que são obrigatórios para usar o processo de incidente declarado. Você pode optar por enviar detalhes adicionais ao Archer. No entanto, os campos listados na tabela a seguir representam a quantidade mínima de dados que você deve enviar.

A tabela a seguir descreve os campos.

| Nome do campo | Tipo de campo |
| --- | --- |
| Título  **Observação:** Este campo é obrigatório. | Texto |
| Resumo do incidente  **Observação:** Este campo é obrigatório. | Texto |
| Detalhes do incidente | Texto |
| Origem | Lista de valores |
| Incidente declarado – Nº de alertas | Numérico |
| Categoria de ameaça | Lista de valores |
| Incidente declarado: Sim  **Observação:** este campo deve ser definido como Sim. | Lista de valores |
| Incidente declarado – Auxiliar: Sim  **Observação:** O Archer inscreve um registro de incidente no workflow avançado de Incidente declarado quando este campo é definido como Sim. | Lista de valores |
| Dispositivo de origem – Contexto de gerenciamento empresarial  **Observação:** este campo permite que você pesquise os IDs de conteúdo do dispositivo existente. | Referência cruzada |
| Dispositivo de destino – Contexto de gerenciamento empresarial  **Observação:** este campo permite que você pesquise os IDs de conteúdo do dispositivo existente. | Referência cruzada |