### パーサーテスト

#### HTTPリクエスト

POST /api/sonar/parsers/:code/test

cURL例

curl -H "Authorization: Bearer <API\_KEY>" \ -d line="<36>[SNIPER-2000] [Attack\_Name=(0023)UDP Check Sum Error], [Time=2013/05/14 14:32:05], [Hacker=130.1.254.133], [Victim=130.1.213.10], [Protocol=udp/514], [Risk=Medium], [Handling=Alarm], [Information=], [SrcPort=514]" \ -X POST \ https://HOSTNAME/api/sonar/parsers/sniper/test

リクエストパラメータ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| キー | 必須 | 型 | 説明 | 備考 |
| code | ○ | 文字列 | パーサー識別子 |  |
| line | ○ | 文字列 | テスト対象の文字列 |  |

#### 正常応答

以下は、cURL例で送信したスナイパーIPSログをパースした結果です。

{ "rows": [ { "time": "2013-05-14 14:32:05+0900", "risk": "MEDIUM", "category": null, "host\_name": "SNIPER-2000", "src\_ip": "130.1.254.133", "src\_port": 514, "dst\_ip": "130.1.213.10", "dst\_port": 514, "protocol": "UDP", "hack\_code": "0023", "signature": "(0023)UDP Check Sum Error", "action": "DETECT" } ]}

* **rows**（配列）：パース結果のレコードリスト。パーサー設定によってフィールドや値の構成は異なります。

#### エラー応答

パーサーが存在しない場合

{ "error\_code": "illegal-state", "error\_msg": "parser profile not found: unknown"}

パースに失敗した場合

パースに失敗した場合は、元のデータをlineフィールドにそのまま返します。

{ "rows": [ { "line": "Hello world," } ]}