### バッチ検出シナリオ一覧取得

検索条件に一致するバッチ検出シナリオの一覧を取得します。

#### HTTPリクエスト

GET /api/sonar/batch-rules

cURL例

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/batch-rules

リクエストパラメータ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| キー | 必須 | 型 | 説明 | 備考 |
| offset | × | 32ビット整数 | スキップする件数 | デフォルトは0 |
| limit | × | 32ビット整数 | 最大取得件数 | 未指定時は全件取得 |
| keywords | × | 文字列 | 検索キーワード | 名前、説明、クエリ対象で検索 |
| category\_guids | × | 文字列リスト | シナリオ分類GUIDリスト | カンマ（,）区切りのGUIDリスト |
| enabled | × | ブール値 | 検出有効化フラグ |  |
| use\_ticket | × | ブール値 | チケット使用フラグ |  |
| use\_explanation | × | ブール値 | 弁明使用フラグ |  |

#### 正常応答

以下はバッチ検出シナリオ一覧の一部例です。

{ "total\_count": 1, "rules": [ { "guid": "f4ca02c8-0679-49e7-8c10-76667c26b595", "priority": "LOW", "name": "DMZポートスキャン", "description": "", "msg": "DMZポートスキャン: $src\_ip", "enabled": false, "category\_guid": "8270a382-a47c-401d-9318-037c5d639f2e", "category\_name": "情報収集", "schedule": "\*/10 \* \* \* \*", "duration": null, "datetrunc": null, "dataset\_guid": null, "dataset\_name": null, "query": "table duration=30m FW\_\*\n| fields \_time, \_schema, src\_ip, src\_port, dst\_ip, dst\_port, protocol, app, action, sent\_pkts, rcvd\_pkts, sent\_bytes, rcvd\_bytes\n| search \_schema == \"session\" and protocol == \"TCP\" and sent\_bytes <= 200\n| lookup geoip src\_ip output country as src\_country\n| lookup geoip dst\_ip output country as dst\_country\n| search src\_country != \"--\"\n| eval \_time = datetrunc(\_time, \"10m\") \n| stats dc(dst\_port) as port\_count, values(dst\_port) as dst\_port by src\_ip, dst\_ip, \_time \n| search port\_count >= 10 \n| explode dst\_port \n| eval protocol = \"TCP\" \n| order \_time, host\_count, src\_ip, dst\_ip, dst\_port, protocol", "address\_group\_guid": null, "address\_field": null, "ticket\_repo\_guid": null, "ticket\_assignee\_guid": null, "ticket\_assignee\_name": null, "ticket\_suppress\_interval": 3600, "event\_suppress\_interval": 0, "suppress\_key": null, "keep\_alive": false, "audit\_category\_guid": null, "audit\_category\_name": null, "auditor\_guid": null, "auditor\_name": null, "audit\_days": 14, "employee\_key\_field": null, "alarm\_group\_guid": null, "alarm\_group\_name": null, "field\_order": "\_time, host\_count, src\_ip, dst\_ip, dst\_port, protocol", "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": null, "user\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "user\_name": "管理者", "created": "2022-09-01 00:31:15+0900", "updated": "2022-09-01 00:31:15+0900" } ]}

* **total\_count**（32ビット整数）：検索条件に一致するバッチ検出シナリオの総件数
* **rules**（配列）：ページングされたバッチ検出シナリオ一覧
* **priority**（文字列）：LOW、MEDIUM、HIGHのいずれか
* **guid**（文字列）：バッチ検出シナリオのGUID
* **name**（文字列）：バッチ検出シナリオ名
* **description**（文字列）：バッチ検出シナリオの説明
* **msg**（文字列）：メッセージテンプレート。$field形式のマクロでフィールド値をメッセージに反映可能
* **enabled**（ブール値）：検出有効化フラグ
* **category\_guid**（文字列）：検出シナリオ分類GUID
* **category\_name**（文字列）：検出シナリオ分類名
* **schedule**（文字列）：実行スケジュール。CRON書式
* **duration**（32ビット整数）：分析対象期間（秒）。設定値はクエリのfrom、toパラメータに渡されます
* **datetrunc**（32ビット整数）：時間切り捨て単位（秒）。from、toクエリパラメータの時間切り捨て
* **dataset\_guid**（文字列）：データセットGUID
* **dataset\_name**（文字列）：データセット名
* **address\_group\_guid**（文字列）：アドレスグループGUID
* **address\_field**（文字列）：アドレスグループに登録する対象フィールド
* **ticket\_repo\_guid**（文字列）：チケット分類GUID
* **ticket\_assignee\_guid**（文字列）：チケット担当者GUID
* **ticket\_assignee\_name**（文字列）：チケット担当者名
* **ticket\_suppress\_interval**（32ビット整数）：重複チケット抑制期間（秒単位）
* **event\_suppress\_interval**（32ビット整数）：重複イベント抑制期間（秒単位）
* **suppress\_key**（文字列）：重複判定キー。$field形式で指定されたマクロを該当フィールド値に置換し、イベントコンテキストキーとして使用
* **keep\_alive**（ブール値）：trueの場合、抑制タイマーを維持。falseの場合、抑制タイマーを初期化
* 抑制タイマーを維持する場合、チケットが完了処理されても有効期限に達するまでイベントは既存チケットに統合されます。
* **audit\_category\_guid**（文字列）：弁明分類GUID
* **audit\_category\_name**（文字列）：弁明分類名
* **auditor\_guid**（文字列）：弁明確認ユーザーのGUID。未指定時は部門長が承認
* **auditor\_name**（文字列）：弁明確認ユーザー名。未指定時は部門長が承認
* **audit\_days**（32ビット整数）：弁明提出期限（日単位）
* **employee\_key\_field**（文字列）：従業員番号フィールド名。通常は正規化フィールドemp\_keyを使用
* **alarm\_group\_guid**（文字列）：アラームグループGUID
* **alarm\_group\_name**（文字列）：アラームグループ名
* **field\_order**（文字列）：エビデンス出力時のフィールド順。カンマ区切りのフィールド名リスト
* **company\_guid**（文字列）：シナリオが属する会社（テナント）GUID
* **company\_name**（文字列）：シナリオが属する会社（テナント）名
* **user\_guid**（文字列）：シナリオ作成ユーザーGUID
* **user\_name**（文字列）：シナリオ作成ユーザー名
* **created**（文字列）：作成日時（yyyy-MM-dd HH:mm:ssZ形式）
* **updated**（文字列）：更新日時（yyyy-MM-dd HH:mm:ssZ形式）

#### エラー応答

offset、limitの値が整数でない場合

HTTPステータスコード 400 応答

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset、limitの値が負の場合

HTTPステータスコード 400 応答

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

シナリオ分類識別子がGUID形式でない場合

HTTPステータスコード 400 応答

{ "error\_code": "invalid-param-type", "error\_msg": "category\_guids should be guid type."}