### ストリーム検出シナリオ一覧取得

検索条件に一致するストリーム検出シナリオの一覧を取得します。

#### HTTPリクエスト

GET /api/sonar/stream-rules

cURL例

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

リクエストパラメータ

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

#### 正常応答

以下はストリーム検出シナリオ一覧の一部例です。

{ "total\_count": 52, "rules": [ { "priority": "LOW", "guid": "3b05608f-8dd0-4218-9d6d-391515b6280d", "name": "Windowsファイアウォール無効化", "description": "(T1089) Disabling Security Tools\n(T1047) Windows Management Instrumentation ", "msg": "Windowsファイアウォール無効化: $primary\_ip", "enabled": false, "category\_guid": "aedc65d6-25ee-4d9e-9040-e21ebe823f8d", "category\_name": "セキュリティ回避", "schema\_code": "edr-process", "schema\_name": "EDRプロセス", "logger\_guids": [], "commands": [ { "template\_id": 1, "field\_name": "", "args": {}, "query": "search (lower(image) == \"\*\\\\netsh.exe\" and lower(cmd\_line) == \"\*advfirewall\*\" and lower(cmd\_line) == \"\*off\*\") or (lower(image) == \"\*\\\\netsh.exe\" and lower(cmd\_line) == \"\*firewall\*\" and lower(cmd\_line) == \"\*disable\*\")", "invert": false, "ordinal": 0 } ], "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": "cmd\_line, image", "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "ログプレッソ", "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ストリーム検出シナリオの総件数
* **rules**（配列）：ページネーションされたストリーム検出シナリオ一覧
* **priority**（文字列）：LOW、MEDIUM、HIGHのいずれか
* **guid**（文字列）：ストリーム検出シナリオのGUID
* **name**（文字列）：ストリーム検出シナリオ名
* **description**（文字列）：ストリーム検出シナリオの説明
* **msg**（文字列）：メッセージテンプレート。$field形式のマクロでフィールド値をメッセージに反映可能
* **enabled**（ブール値）：検出有効化フラグ
* **category\_guid**（文字列）：検出シナリオ分類GUID
* **category\_name**（文字列）：検出シナリオ分類名
* **schema\_code**（文字列）：正規化スキーマ識別子
* **schema\_name**（文字列）：正規化スキーマ名
* **logger\_guids**（配列）：ロガーGUIDリスト
* **commands**（配列）：ストリーム検出シナリオコマンド一覧
* **template\_id**（32ビット整数）：ストリーム検出シナリオコマンドテンプレートID
* **field\_name**（文字列）：対象フィールド名
* **args**（マップ）：引数のキー／値ペア
* **query**（文字列）：引数が反映されたクエリ文字列
* **invert**（ブール値）：trueの場合はNOT条件
* **ordinal**（32ビット整数）：順序
* **address\_group\_guid**（文字列）：アドレスグループGUID
* **address\_field**（文字列）：アドレスグループに登録する対象フィールド
* **ticket\_repo\_guid**（文字列）：チケット分類GUID
* **ticket\_assignee\_guid**（文字列）：チケット担当者GUID
* **ticket\_assignee\_name**（文字列）：チケット担当者名
* **ticket\_suppress\_interval**（32ビット整数）：重複チケット抑制期間（秒単位）
* **event\_suppress\_interval**（32ビット整数）：重複イベント抑制期間（秒単位）
* **suppress\_key**（文字列）：重複判定用フィールド。$field形式の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利用
* **keep\_alive**（ブール値）：trueの場合は抑制タイマーを維持、falseの場合は抑制タイマーを初期化
* 抑制タイマーを維持する場合、チケットを完了処理し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の値が負の値の場合

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."}