### ストリーム検出シナリオの作成

新しいストリーム検出シナリオを作成します。

#### HTTPリクエスト

POST /api/sonar/stream-rules

cURL例

curl -H "Authorization: Bearer <API\_KEY>" \ -d priority="HIGH" \ -d name="既知ボットネット帯域への接続" \ -d msg="既知ボットネット帯域への接続: $dst\_ip" \ -d schema\_code="session" \ -d commands="[{'template\_id': 3, 'query': 'matchnet invert=t field=dst\_ip guid=697393b6-aecf-4e9d-a32c-8724cd8f067e verify=f', 'field\_name': 'dst\_ip', 'args':{'subnet':'697393b6-aecf-4e9d-a32c-8724cd8f067e'}}]" \ -X POST \ 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 |
| priority | ○ | 文字列 | 重要度 | LOW, MEDIUM, HIGH のいずれか |
| guid | × | 文字列 | ストリーム検出シナリオGUID | 36文字 |
| name | ○ | 文字列 | ストリーム検出シナリオ名 | 最小1文字、最大255文字 |
| description | × | 文字列 | ストリーム検出シナリオ説明 | 最大2,000文字 |
| msg | ○ | 文字列 | メッセージテンプレート | 最小1文字、最大2,000文字 |
| enabled | × | ブール値 | 有効化フラグ | true または false |
| category\_guid | × | 文字列 | シナリオ分類GUID | 36文字 |
| schema\_code | ○ | 文字列 | 正規化スキーマ識別子 | 最小1文字、最大50文字 |
| logger\_guids | ○ | 配列 | ロガーGUIDリスト |  |
| commands | ○ | 配列 | ストリーム検出コマンドリスト | 1つ以上のコマンドが必要。下記説明参照 |
| address\_group\_guid | × | 文字列 | アドレスグループGUID | 36文字 |
| address\_field | × | 文字列 | アドレスフィールド | アドレスグループに登録するフィールド名。最大50文字 |
| ticket\_repo\_guid | × | 文字列 | チケット分類GUID | 未設定時はチケット発生なし。36文字 |
| ticket\_assignee\_guid | × | 文字列 | チケット担当者GUID | 指定時は担当者を自動割当 |
| ticket\_suppress\_interval | × | 32ビット整数 | 重複チケット抑制期間 | 秒単位。0または未設定時は同一チケットを統合しない |
| event\_suppress\_interval | × | 32ビット整数 | 重複イベント除外期間 | 秒単位。0または未設定時は重複イベントを除外しない |
| suppress\_key | × | 文字列 | 重複判定キー | $field形式でマクロ利用可。最大2,000文字 |
| keep\_alive | × | ブール値 | 抑制タイマー維持フラグ | 抑制タイマー維持時はtrue、初期化時はfalse |
| audit\_category\_guid | × | 文字列 | 弁明分類GUID | 未設定時は自動弁明リクエストが無効。36文字 |
| auditor\_guid | × | 文字列 | 弁明確認ユーザーGUID | 未設定時は部門長が承認。36文字 |
| audit\_days | × | 32ビット整数 | 弁明提出期限 | 最小1日、最大365日 |
| employee\_key\_field | × | 文字列 | 従業員番号フィールド名 | 未設定時は自動弁明リクエストが無効。最大50文字 |
| alarm\_group\_guid | × | 文字列 | アラームグループGUID | 36文字 |
| field\_order | × | 文字列 | エビデンスフィールド出力順 | 最大2,000文字 |

commandsの各配列要素は以下のように定義します：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| キー | 必須 | 型 | 説明 | 備考 |
| template\_id | ○ | 32ビット整数 | ストリーム検出コマンドテンプレートID |  |
| query | ○ | 文字列 | 部分クエリ文字列 |  |
| field\_name | × | 文字列 | 対象フィールド名 |  |
| args | × | マップ | 引数キー/値 |  |
| invert | × | ブール値 | 反転フラグ |  |

#### 正常応答

{}

#### エラー応答

必須パラメータが不足している場合

HTTPステータスコード 400 応答

{ "error\_code": "null-argument", "error\_msg": "schema\_code should be not null"}

パラメータ値の長さが不正な場合

HTTPステータスコード 400 応答

{ "error\_code": "invalid-argument", "error\_msg": "'schema\_code' must be shorter than or equal to 50 characters."}

不正な重要度値を使用した場合

HTTPステータスコード 400 応答

{ "error\_code": "invalid-argument", "error\_msg": "priority should be one of 'LOW', 'MEDIUM', 'HIGH'."}

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\_guid should be guid type."}

ストリーム検出コマンドリストが有効なJSON形式でない場合

HTTPステータスコード 400 応答

{ "error\_code": "invalid-argument", "error\_msg": "'commands' parameter should follow valid JSON syntax"}

正規化スキーマが存在しない場合

HTTPステータスコード 500 応答

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

シナリオ作成権限がない場合

HTTPステータスコード 500 応答

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}