### バッチ検出シナリオの作成

新しいバッチ検出シナリオを作成します。

#### HTTPリクエスト

POST /api/sonar/batch-rules

cURL例

curl -H "Authorization: Bearer <API\_KEY>" \ -d priority="LOW" \ -d name="ウェブ脆弱性スキャン" \ -d schedule="\*/30 \* \* \* \*" -d msg="ウェブ脆弱性スキャン: $dst\_ip" \ -d query="table duration=30m weblog | search status >= 400 | stats count as error\_count, dc(path) as page\_count, values(concat(method, \" \", path)) as request by src\_ip | eval request = strjoin(\"\n\", request) | lof eps=0.1 error\_count, page\_count | search \_lof > 1.5 | sort -\_lof" \ -X POST \ 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 |
| priority | ○ | 文字列 | 重要度 | LOW, MEDIUM, HIGH のいずれか |
| guid | × | 文字列 | バッチ検出シナリオGUID | 36文字 |
| name | ○ | 文字列 | バッチ検出シナリオ名 | 最小1文字、最大255文字 |
| description | × | 文字列 | バッチ検出シナリオ説明 | 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 |
| schedule | ○ | 文字列 | 実行スケジュール | CRONスケジュール構文を使用 |
| duration | × | 32ビット整数 | 分析対象期間 | 秒単位で指定。最大 31536000 秒（365日） |
| datetrunc | × | 32ビット整数 | 時間切り捨て | 1, 60, 3600, 86400 のいずれか（秒単位） |
| dataset\_guid | × | 文字列 | データセットGUID | dataset\_guidまたはqueryのいずれかは必須。36文字 |
| query | × | 文字列 | 検出クエリ | dataset\_guidまたはqueryのいずれかは必須。最大65535文字 |
| 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り当て |
| 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 | 重複イベント除去期間 | 秒単位。0または未設定時は重複イベントを除去しない |
| suppress\_key | × | 文字列 | 重複判定基準フィールド | $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 |

#### 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": "schedule 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": "'address\_field' 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."}

スケジュールCRON構文が不正な場合

HTTPステータスコード 400 応答

{ "error\_code": "invalid-argument", "error\_msg": "schedule has wrong cron expression format: \* \* \* \* \* \*"}

データセットとクエリの両方が指定されていない場合

HTTPステータスコード 400 応答

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

時間切り捨て値が無効な場合

HTTPステータスコード 400 応答

{ "error\_code": "invalid-argument", "error\_msg": "datetrunc should be one of 1 (1 second), 60 (1 minute), 3600 (1 hour), 86400 (1 day)."}

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"}