### ストリーム検出シナリオ参照

指定したストリーム検出シナリオを参照します。

#### HTTPリクエスト

GET /api/sonar/stream-rules/:guid

cURL例

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/stream-rules/3b05608f-8dd0-4218-9d6d-391515b6280d

リクエストパラメータ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| キー | 必須 | 型 | 説明 | 備考 |
| guid | ○ | 文字列 | ストリーム検出シナリオのGUID | 36桁 |

#### 正常応答

{ "rule": { "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" }}

* **rule**（マップ）: ストリーム検出シナリオ
* **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。$field形式のマクロでフィールド値をメッセージに反映可能
* **enabled**（ブール値）: 検出有効化状態
* **category\_guid**（文字列）: シナリオ分類GUID
* **category\_name**（文字列）: シナリオ分類名
* **schema\_code**（文字列）: 正規化スキーマ識別子
* **schema\_name**（文字列）: 正規化スキーマ名
* **logger\_guids**（配列）: ロガーGUIDリスト
* **commands**（配列）: ストリーム検出シナリオコマンドリスト
* **template\_id**（32ビット整数）: コマンドテンプレートID
* **field\_name**（文字列）: 対象フィールド名
* **args**（マップ）: 引数のキー/値ペア
* **query**（文字列）: 引数が反映されたクエリ文字列
* **invert**（ブール値）: trueの場合はNOT条件
* **ordinal**（32ビット整数）: 順序
* **address\_group\_guid**（文字列）: アドレスグループGUID
* **address\_field**（文字列）: アドレスグループに登録する対象フィールド
* **ticket\_repo\_guid**（文字列）: チケット分類GUID
* **ticket\_assignee\_guid**（文字列）: チケット担当者GUID
* **ticket\_assignee\_name**（文字列）: チケット担当者名
* **ticket\_suppress\_interval**（32ビット整数）: 重複チケット抑制期間（秒単位）
* **event\_suppress\_interval**（32ビット整数）: 重複イベント抑制期間（秒単位）
* **suppress\_key**（文字列）: 重複判定基準フィールド。$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使用
* **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リセット
* 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の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

指定したシナリオが存在しない場合

HTTPステータスコード 200 応答

{ "rule": null}

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": "guid should be guid type."}