### Get Stream Rules

Gets a list of the stream rules that match the search keyword.

#### HTTP Request

GET /api/sonar/stream-rules

Request using cURL

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

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| offset | X | 32-bit integer | Number of records to skip | Default: 0 |
| limit | X | 32-bit integer | Maximum number of records to load | If not specified, load all records |
| keywords | X | String | Keyword | Search available by name, description, query target |

#### Success Response

Below is a portion of the full list of stream rules.

{ "total\_count": 52, "rules": [ { "priority": "LOW", "guid": "3b05608f-8dd0-4218-9d6d-391515b6280d", "name": "Disabling Windows Firewall", "description": "(T1089) Disabling Security Tools\n(T1047) Windows Management Instrumentation ", "msg": "Disabling Windows Firewall: $primary\_ip", "enabled": false, "category\_guid": "aedc65d6-25ee-4d9e-9040-e21ebe823f8d", "category\_name": "Evasion", "schema\_code": "edr-process", "schema\_name": "EDR Processs", "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": "Logpresso", "user\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "user\_name": "Admin", "created": "2022-09-01 00:31:15+0900", "updated": "2022-09-01 00:31:15+0900" } ]}

* **total\_count** (32-bit integer): Total number of stream rules that match the search keyword
* **rules** (Array): Paged list of stream rules
* **priority** (String): One of the following: LOW, MEDIUM, HIGH.
* **guid** (String): Stream rule GUID
* **name** (String): Stream rule name
* **description** (String): Stream rule description
* **msg** (String): Message template. Macro in the $field format available.
* **enabled** (Boolean): Whether the rule is enabled or not
* **category\_guid** (String): Stream rule category GUID
* **category\_name** (String): Stream rule category name
* **schema\_code** (String): Log schema code
* **schema\_name** (String): Log schema name
* **logger\_guids** (Array): Logger GUID list
* **commands** (Array): List of stream rule commands
* **template\_id** (32-bit integer): Stream rule command template ID
* **field\_name** (String): Target field name
* **args** (Map): Argument key/value pairs
* **query** (String): Query string with arguments
* **invert** (Boolean): NOT condition when invert = true
* **ordinal** (32-bit integer): Order
* **address\_group\_guid** (String): Address group GUID
* **address\_field** (String): Target fields to add to the address group
* **ticket\_repo\_guid** (String): Ticket repository GUID
* **ticket\_assignee\_guid** (String): Ticket assignee GUID
* **ticket\_assignee\_name** (String): Ticket assignee name
* **ticket\_suppress\_interval** (32-bit integer): Suppression period for duplicated ticket in seconds (in seconds)
* **event\_suppress\_interval** (32-bit integer): Suppression period for duplicated event in seconds (in seconds)
* **suppress\_key** (String): Suppress key field. Macro in the $field format available.
* **keep\_alive** (Boolean): true to keep the timer alive, false to reset it.
* When keeping the suppression timer, even if a user completes the ticket, the event will be merged into the existing ticket until the expiration time is reached.
* **audit\_category\_guid** (String): Audit category GUID
* **audit\_category\_name** (String): Audit category name
* **auditor\_guid** (String): Auditor GUID. If not specified, the department head is assigned as default.
* **auditor\_name** (String): Auditor name. If not specified, the department head is assigned as default.
* **audit\_days** (32-bit integer): Audit due date (days)
* **employee\_key\_field** (String): Employee number field. Typically using a normalized emp\_key field.
* **alarm\_group\_guid** (String): Alarm group GUID
* **alarm\_group\_name** (String): Alarm group name
* **field\_order** (String): Evidence file output order. Comma-separated list of field names.
* **company\_guid** (String): GUID of the company (tenant) to which the stream rule belongs
* **company\_name** (String): Name of the company (tenant) to which the stream rule belongs
* **user\_guid** (String): GUID of the user who creates the stream rule
* **user\_name** (String): Name of the user who creates the stream rule
* **created** (String): Date and time of creation (yyyy-MM-dd HH:mm:ssZ)
* **updated** (String): Date and time of last modification (yyyy-MM-dd HH:mm:ssZ)

#### Error Responses

offset or limit value is not an integer

HTTP status code 400

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

offset or limit value is negative

HTTP status code 400

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