### Get Batch Rules

Gets a list of batch rules that match the specified search keyword.

#### HTTP Request

GET /api/sonar/batch-rules

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/batch-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 | Keywords | Search available by name, description, query target |

#### Success Response

Below is a partial list of batch rules.

{ "total\_count": 1, "rules": [ { "guid": "f4ca02c8-0679-49e7-8c10-76667c26b595", "priority": "LOW", "name": "DMZ 포트 스캔", "description": "", "msg": "DMZ 포트 스캔: $src\_ip", "enabled": false, "category\_guid": "8270a382-a47c-401d-9318-037c5d639f2e", "category\_name": "정보 수집", "schedule": "\*/10 \* \* \* \*", "duration": null, "datetrunc": null, "dataset\_guid": null, "dataset\_name": null, "query": "table duration=30m FW\_\*\n| fields \_time, \_schema, src\_ip, src\_port, dst\_ip, dst\_port, protocol, app, action, sent\_pkts, rcvd\_pkts, sent\_bytes, rcvd\_bytes\n| search \_schema == \"session\" and protocol == \"TCP\" and sent\_bytes <= 200\n| lookup geoip src\_ip output country as src\_country\n| lookup geoip dst\_ip output country as dst\_country\n| search src\_country != \"--\"\n| eval \_time = datetrunc(\_time, \"10m\") \n| stats dc(dst\_port) as port\_count, values(dst\_port) as dst\_port by src\_ip, dst\_ip, \_time \n| search port\_count >= 10 \n| explode dst\_port \n| eval protocol = \"TCP\" \n| order \_time, host\_count, src\_ip, dst\_ip, dst\_port, protocol", "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": "\_time, host\_count, src\_ip, dst\_ip, dst\_port, protocol", "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": null, "user\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "user\_name": "관리자", "created": "2022-09-01 00:31:15+0900", "updated": "2022-09-01 00:31:15+0900" } ]}

* **total\_count** (32-bit integer): Total number of the batch rules that match the search keyword.
* **rules** (Array): Paged list of batch rules
* **priority** (String): LOW or MEDIUM or HIGH
* **guid** (String): Batch Rule GUID
* **name** (String): Batch Rule name
* **description** (String): Batch rule description
* **msg** (String): Message template. Macro in the $field format available.
* **enabled** (Boolean): Whether the rule is enabled or not
* **category\_guid** (String): Batch rule category GUID
* **category\_name** (String): Batch rule category name
* **schedule** (String): Execution schedule in CRON schedule format
* **duration** (32-bit integer): Time window of the data to be analyzed, based on the current time (in seconds). The value is passed to the from and to parameters of the query.
* **datetrunc** (32-bit integer): Date truncation unit (in seconds). Date truncation unit for the from, to parameters of the query.
* **dataset\_guid** (String): Dataset GUID
* **dataset\_name** (String): Dataset name
* **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 batch rule belongs
* **company\_name** (String): Name of the company (tenant) to which the batch rule belongs
* **user\_guid** (String): GUID of the user who creates the batch rule
* **user\_name** (String): Name of the user who creates the batch 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."}