### Create Batch Rule

Creates a new batch rule.

#### HTTP Request

POST /api/sonar/batch-rules

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d priority="LOW" \ -d name="Scan web vulnerabilities" \ -d schedule="\*/30 \* \* \* \*" -d msg="Scan web vulnerabilities: $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

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| priority | O | String | Priority | LOW or MEDIUM or HIGH |
| guid | X | String | Batch rule GUID | 36 characters |
| name | O | String | Batch rule name | Minimum 1 to maximum 255 characters |
| description | X | String | Batch rule description | Maximum 2,000 characters |
| msg | O | String | Message template | Minimum 1 to maximum 2,000 characters |
| enabled | X | Boolean | Whether the batch rule is enabled | true or false |
| category\_guid | X | String | Batch rule category GUID | 36 characters |
| schedule | O | String | Execution cycle | CRON schedule format |
| duration | X | 32-bit integer | Time window of the data to be analyzed, based on the current time | Up to 31536000 seconds (365 days) |
| datetrunc | X | 32-bit integer | Date truncation unit | 1 or 60 or 3600 or 86400 (seconds) |
| dataset\_guid | X | String | Dataset GUID | 36 character. At least one of dataset\_guid and query must be provided. |
| query | X | String | Detection query | Maximum 65,535 characters. At least one of dataset\_guid and query must be provided. |
| address\_group\_guid | X | String | Address group GUID | 36 characters |
| address\_field | X | String | Address field name | Address group field name. Maximum 50 characters. |
| ticket\_repo\_guid | X | String | Ticket repository GUID | 36 characters. If not specified, a ticket is not generated. |
| ticket\_assignee\_guid | X | String | Ticket assignee GUID | If specified, a ticket is assigned automatically. |
| ticket\_suppress\_interval | X | 32-bit integer | Suppression period for duplicate ticket (in seconds) | If set to 0 or not specified, duplicate tickets are not merged. |
| event\_suppress\_interval | X | 32-bit integer | Suppression period for duplicated event (in seconds) | If set to 0 or not specified, duplicate events are not merged. |
| suppress\_key | X | String | Suppress key field | Maximum 2,000 characters. Macro in $field format available. |
| keep\_alive | X | Boolean | Whether to keep the suppression timer alive | true to keep the timer alive, false to reset it. |
| audit\_category\_guid | X | String | Audit category GUID | 36 characters. If not specified, an auto audit request is not sent. |
| auditor\_guid | X | String | Auditor GUID | 36 characters. If not specified, the department head is assigned as default. |
| audit\_days | X | 32-bit integer | Audit due date | Minimum 1 to maximum 365 days |
| employee\_key\_field | X | String | Employee number field | Maximum 50 characters. If not specified, an auto audit request is not sent. |
| alarm\_group\_guid | X | String | Alarm group GUID | 36 characters |
| field\_order | X | String | Evidence field output order | Maximum 2,000 characters |

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400

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

Invalid argument length

HTTP status code 400

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

Invalid priority value

HTTP status code 400

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

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "category\_guid should be guid type."}

CRON expression is not valid

HTTP status code 400

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

Both dataset and query are not specified

HTTP status code 400

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

Invalid date truncation unit value

HTTP status code 400

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

No privilege to create a batch rule

HTTP status code 500

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