### Get Ticket

Retrieves information of a specified ticket.

#### HTTP Request

GET /api/sonar/tickets/:guid

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/tickets/49272877-75f2-4c2f-9301-d21c4f9a106d

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Ticket GUID | 36 characters |

#### Success Response

{ "ticket": { "id": 2, "repo\_guid": "5f0ba741-7551-400d-8bd6-1f14a6e8536d", "repo\_name": "Threat", "guid": "49272877-75f2-4c2f-9301-d21c4f9a106d", "title": "Attempt to collect web server settings: 20.0.31.172", "priority": "LOW", "status": "APPROVED", "format": "JSON", "rule\_guid": "ad4b9871-d5f0-4a8b-a341-8ac0afcdcddf", "rule\_type": "STREAM", "rule\_name": "Attempt to collect web server settings", "count": 7, "content": "{\"first\_seen\":\"2022-09-14 17:34:19+0900\",\"last\_seen\":\"2022-09-14 23:55:29+0900\",\"priority\":\"LOW\",\"rule\_type\":\"STREAM\",\"rule\_id\":27,\"src\_ip\":\"20.0.31.172\",\"src\_port\":null,\"dst\_ip\":null,\"dst\_port\":null,\"protocol\":null,\"action\":null,\"count\":1,\"msg\":\"웹 서버 설정 수집 시도: 20.0.31.172\",\"user\":null,\"host\_ip\":null,\"mail\_from\":null,\"mail\_to\":null,\"mail\_cc\":null,\"logger\_id\":28,\"logger\_name\":\"ko.logpresso.com \",\"field\_order\":\"\_time, src\_ip, src\_port, dst\_ip, dst\_port, status, method, path, query, user\_agent\",\"url\":null,\"md5\":null,\"src\_asn\":\"AS8075 Microsoft Corporation\",\"src\_country\":\"US\",\"src\_city\":null,\"src\_lat\":37.750999450683594,\"src\_lng\":-97.8219985961914}", "attack": true, "incident": false, "assignees": [ { "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "Logpresso", "user\_guid": "bfd00bb0-be99-4fd5-8380-166f544975fa", "user\_name": "Joshua", "task\_type": "ASSIGNEE", "task\_status": "CLOSED", "x\_login": null, "x\_user": null, "x\_dept": null } ], "approvers": [ { "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "Logpresso", "user\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "user\_name": "Jerry", "task\_type": "APPROVER", "task\_status": "APPROVED", "x\_login": null, "x\_user": null, "x\_dept": null } ], "attachments": [ { "guid": "d4390b7a-7d64-4a24-bd3e-af74b4f3c204", "user\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "ticket\_guid": "49272877-75f2-4c2f-9301-d21c4f9a106d", "file\_name": "3bc31b3d-bc25-4be5-8dae-d3cb1831da02.png", "file\_size": 124118 } ], "created": "2022-09-14 17:34:19+0900", "updated": "2022-09-14 23:55:29+0900", "closed": null, "x\_login": null, "x\_user": null, "x\_dept": null, "comments": [ { "guid": "b66a31b5-db94-478b-8751-194b5ee5f358", "user\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "user\_name": "Joshua", "type": "TEXT", "format": "MARKDOWN", "content": "\* Blocked the IP address in firewall.", "created": "2022-09-14 23:57:34+0900", "updated": "2022-09-14 23:57:34+0900", "x\_login": null, "x\_user": null, "x\_dept": null } ] }}

* (Map) ticket
* **id** (32-bit integer): Ticket ID
* **repo\_guid** (String): Ticket type GUID
* **repo\_name** (String): Ticket type name
* **site\_guid** (String): Site GUID
* **site\_name** (String): Site name
* **guid** (String): Ticket GUID
* **title** (String): Ticket title
* **priority** (String): Ticket priority. One of the following: HIGH, MEDIUM, LOW.
* **status** (String): Ticket status. One of the following: NEW, ASSIGNED, IN\_PROGRESS, SUBMITTED, APPROVED, REJECTED, CLOSED.
* **format** (String): Ticket format. One of the following: JSON, MARKDOWN, PLAIN. Threat detection ticket uses JSON format.
* **rule\_guid** (String): Detection rule GUID
* **rule\_type** (String): Detection rule type. STREAM or BATCH.
* **rule\_name** (String): Detection rule name
* **count** (32-bit integer): Number of merged duplicate tickets
* **content** (String): Ticket data. The Event field is written in JSON format for threat detection tickets.
* **attack** (Boolean): Whether the detection is false or not, recorded after analysis. Logged as true if the detection is true
* **incident** (Boolean): Whether an incident occurred or not, recorded after analysis. Recorded as true if the incident requires an immediate response, such as an endpoint infection.
* **assignees** (Array): Ticket assignee list
* **company\_guid** (String): Company (tenant) GUID
* **company\_name** (String): Company (tenant) name
* **user\_guid** (String): Assignee GUID
* **user\_name** (String): Assignee name
* **task\_type** (String): Always ASSIGNEE
* **task\_status** (String): ASSIGNED or IN\_PROGRESS or CLOSED
* **x\_login** (String): Login user name logged when the assignee account is deleted
* **x\_user** (String): User name logged when the assignee account is deleted
* **x\_dept** (String): Department name logged when the assignee account is deleted
* **approvers** (Array): Ticket approver list
* **company\_guid** (String): Company (tenant) GUID
* **company\_name** (String): Company (tenant) name
* **user\_guid** (String): Approver GUID
* **user\_name** (String): Approver name
* **task\_type** (String): Always APPROVER
* **task\_status** (String): ASSIGNED or IN\_PROGRESS or CLOSED
* **x\_login** (String): Login user name logged when the approver account is deleted
* **x\_user** (String): User name logged when the approver account is deleted
* **x\_dept** (String): Department name logged when the approver account is deleted
* **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)
* **closed** (String): Date and time of ticket closing (yyyy-MM-dd HH:mm:ssZ)
* **x\_login** (String): Login user name logged when the ticket author account is deleted
* **x\_user** (String): User name logged when the ticket author account is deleted
* **x\_dept** (String): Department name logged when the ticket author account is deleted
* **x\_site** (String): Site name logged when the site is deleted
* **comments** (Array): Ticket comment list
* **guid** (String): Ticket comment GUID
* **user\_guid** (String): Ticket author GUID
* **user\_name** (String): Ticket author name
* **type** (String): Always TEXT
* **format** (String): Markdown (MARKDOWN) or plain text (PLAIN)
* **content** (String): Comment content
* **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)
* **x\_login** (String): Login user name logged when logged when the ticket comment author account is deleted
* **x\_user** (String): User name logged when logged when the ticket comment author account is deleted
* **x\_dept** (String): Department name logged when logged when the ticket comment author account is deleted

#### Error Responses

Ticket is not found

HTTP status code 200

{ "ticket": null}

Ticket identifier is not in valid GUID format

HTTP status code 400

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