### チケット照会

指定したチケットを照会します。

#### HTTPリクエスト

GET /api/sonar/tickets/:guid

cURL例

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

リクエストパラメータ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| キー | 必須 | 型 | 説明 | 備考 |
| guid | ○ | 文字列 | チケットGUID | 36文字 |

#### 正常応答

{ "ticket": { "id": 2, "repo\_guid": "5f0ba741-7551-400d-8bd6-1f14a6e8536d", "repo\_name": "脅威分析", "guid": "49272877-75f2-4c2f-9301-d21c4f9a106d", "title": "Webサーバー設定収集試行: 20.0.31.172", "priority": "LOW", "status": "APPROVED", "format": "JSON", "rule\_guid": "ad4b9871-d5f0-4a8b-a341-8ac0afcdcddf", "rule\_type": "STREAM", "rule\_name": "Webサーバー設定収集試行", "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\":\"Webサーバー設定収集試行: 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": "ログプレッソ", "user\_guid": "bfd00bb0-be99-4fd5-8380-166f544975fa", "user\_name": "ク・ドンオン", "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": "ログプレッソ", "user\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "user\_name": "ホン・ギルドン", "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": "ホン・ギルドン", "type": "TEXT", "format": "MARKDOWN", "content": "\* ファイアウォールでIPをブロック", "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 } ] }}

* (マップ) ticket
* **id** (32ビット整数): チケットID
* **repo\_guid** (文字列): チケット種別識別子
* **repo\_name** (文字列): チケット種別名
* **site\_guid** (文字列): サイト識別子
* **site\_name** (文字列): サイト名
* **guid** (文字列): チケット識別子
* **title** (文字列): タイトル
* **priority** (文字列): 重要度。高（HIGH）、中（MEDIUM）、低（LOW）のいずれか。
* **status** (文字列): 状態。新規（NEW）、割当済み（ASSIGNED）、処理中（IN\_PROGRESS）、承認申請中（SUBMITTED）、承認（APPROVED）、却下（REJECTED）、完了（CLOSED）のいずれか。
* **format** (文字列): チケット形式。JSON、MARKDOWN、PLAINのいずれか。脅威検知チケットはJSON形式で情報が記録されます。
* **rule\_guid** (文字列): 検出シナリオ識別子
* **rule\_type** (文字列): 検出シナリオタイプ。STREAMまたはBATCHのいずれか。
* **rule\_name** (文字列): 検出シナリオ名
* **count** (32ビット整数): 重複集約件数
* **content** (文字列): チケットデータ。脅威検知チケットの場合、イベントフィールドがJSON形式で記録されます。
* **attack** (ブール値): 分析後に記録された真陽性判定。検知が正確であればtrueとなります。
* **incident** (ブール値): 分析後に記録されたインシデント発生有無。エンドポイント感染など即時対応が必要な場合はtrueとなります。
* **assignees** (配列): チケット担当者リスト
* **company\_guid** (文字列): 会社（テナント）識別子
* **company\_name** (文字列): 会社（テナント）名
* **user\_guid** (文字列): 担当者ユーザー識別子
* **user\_name** (文字列): 担当者氏名
* **task\_type** (文字列): ASSIGNEE固定
* **task\_status** (文字列): 割当済み（ASSIGNED）、処理中（IN\_PROGRESS）、完了（CLOSED）のいずれか
* **x\_login** (文字列): 担当者アカウント削除時に記録されるログインアカウント名
* **x\_user** (文字列): 担当者アカウント削除時に記録されるユーザー氏名
* **x\_dept** (文字列): 担当者アカウント削除時に記録される部署名
* **approvers** (配列): チケット承認者リスト
* **company\_guid** (文字列): 会社（テナント）識別子
* **company\_name** (文字列): 会社（テナント）名
* **user\_guid** (文字列): 承認者ユーザー識別子
* **user\_name** (文字列): 承認者氏名
* **task\_type** (文字列): APPROVER固定
* **task\_status** (文字列): 割当済み（ASSIGNED）、承認（APPROVED）、却下（REJECTED）のいずれか
* **x\_login** (文字列): 承認者アカウント削除時に記録されるログインアカウント名
* **x\_user** (文字列): 承認者アカウント削除時に記録されるユーザー氏名
* **x\_dept** (文字列): 承認者アカウント削除時に記録される部署名
* **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
* **closed** (文字列): 完了日時。yyyy-MM-dd HH:mm:ssZ形式
* **x\_login** (文字列): チケット作成アカウント削除時に記録されるログインアカウント名
* **x\_user** (文字列): チケット作成アカウント削除時に記録されるユーザー氏名
* **x\_dept** (文字列): チケット作成アカウント削除時に記録される部署名
* **x\_site** (文字列): サイト削除時に記録されるサイト名
* **comments** (配列): チケットメモリスト
* **guid** (文字列): チケットメモ識別子
* **user\_guid** (文字列): メモ作成者識別子
* **user\_name** (文字列): メモ作成者氏名
* **type** (文字列): TEXT固定
* **format** (文字列): マークダウン（MARKDOWN）、プレーンテキスト（PLAIN）のいずれか
* **content** (文字列): メモ内容
* **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
* **x\_login** (文字列): メモ作成アカウント削除時に記録されるログインアカウント名
* **x\_user** (文字列): メモ作成アカウント削除時に記録されるユーザー氏名
* **x\_dept** (文字列): メモ作成アカウント削除時に記録される部署名

#### エラー応答

チケットが存在しない場合

HTTPステータスコード 200 応答

{ "ticket": null}

チケット識別子が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."}