### 티켓 조회

지정한 티켓을 조회합니다.

#### HTTP 요청

GET /api/sonar/tickets/:guid

cURL 예시

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

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 티켓 GUID | 36자 |

#### 정상 응답

{ "ticket": { "id": 2, "repo\_guid": "5f0ba741-7551-400d-8bd6-1f14a6e8536d", "repo\_name": "위협분석", "guid": "49272877-75f2-4c2f-9301-d21c4f9a106d", "title": "웹 서버 설정 수집 시도: 20.0.31.172", "priority": "LOW", "status": "APPROVED", "format": "JSON", "rule\_guid": "ad4b9871-d5f0-4a8b-a341-8ac0afcdcddf", "rule\_type": "STREAM", "rule\_name": "웹 서버 설정 수집 시도", "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": "로그프레소", "user\_guid": "bfd00bb0-be99-4fd5-8380-166f544975fa", "user\_name": "구동언", "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": "로그프레소", "user\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "user\_name": "양봉열", "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": "양봉열", "type": "TEXT", "format": "MARKDOWN", "content": "\* 방화벽에서 IP 차단함", "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 } ] }}

* (맵) ticket
* **id** (32비트 정수): 티켓 ID
* **repo\_guid** (문자열): 티켓 유형 식별자
* **repo\_name** (문자열): 티켓 유형 이름
* **site\_guid** (문자열): 사이트 식별자
* **site\_name** (문자열): 사이트 이름
* **guid** (문자열): 티켓 식별자
* **title** (문자열): 제목
* **priority** (문자열): 중요도. 상 (HIGH), 중 (MEDIUM), 하 (LOW) 중 하나.
* **status** (문자열): 상태. 신규 (NEW), 할당 (ASSIGNED), 처리중 (IN\_PROGRESS), 결재중 (SUBMITTED), 승인 (APPROVED), 반려 (REJECTED), 완료 (CLOSED) 중 하나.
* **format** (문자열): 티켓 형식. JSON, MARKDOWN, PLAIN 중 하나. 위협 탐지 티켓은 JSON 형식으로 정보 기록.
* **rule\_guid** (문자열): 탐지 시나리오 식별자
* **rule\_type** (문자열): 탐지 시나리오 유형. STREAM, BATCH 중 하나.
* **rule\_name** (문자열): 탐지 시나리오 이름
* **count** (32비트 정수): 중복 축약 건수.
* **content** (문자열): 티켓 데이터. 위협 탐지 티켓은 이벤트 필드가 JSON 형식으로 기록됨.
* **attack** (불리언): 분석 후 기록한 정탐 여부. 탐지 자체가 정확하다면 true로 기록함.
* **incident** (불리언): 분석 후 기록한 사고 발생 여부. 엔드포인트 감염 발생 등 즉각적 대응이 필요한 상황인 경우 true로 기록함.
* **assignees** (배열): 티켓 할당자 목록
* **company\_guid** (문자열): 회사 (테넌트) 식별자
* **company\_name** (문자열): 회사 (테넌트) 이름
* **user\_guid** (문자열): 할당자 계정 식별자
* **user\_name** (문자열): 할당자 성명
* **task\_type** (문자열): ASSIGNEE 고정.
* **task\_status** (문자열): 할당 (ASSIGNED), 처리중 (IN\_PROGRESS), 완료 (CLOSED) 중 하나.
* **x\_login** (문자열): 할당자 계정 삭제 시 기록되는 로그인 계정 이름
* **x\_user** (문자열): 할당자 계정 삭제 시 기록되는 사용자 성명
* **x\_dept** (문자열): 할당자 계정 삭제 시 기록되는 부서 이름
* **approvers** (배열): 티켓 결재자 목록
* **company\_guid** (문자열): 회사 (테넌트) 식별자
* **company\_name** (문자열): 회사 (테넌트) 이름
* **user\_guid** (문자열): 결재자 계정 식별자
* **user\_name** (문자열): 결재자 성명
* **task\_type** (문자열): APPROVER 고정.
* **task\_status** (문자열): 할당 (ASSIGNED), 승인 (ASSIGNED), 반려 (REJECTED) 중 하나.
* **x\_login** (문자열): 결재자 계정 삭제 시 기록되는 로그인 계정 이름
* **x\_user** (문자열): 결재자 계정 삭제 시 기록되는 사용자 성명
* **x\_dept** (문자열): 결재자 계정 삭제 시 기록되는 부서 이름
* **created** (문자열): 생성일시. yyyy-MM-dd HH:mm:ssZ 형식
* **updated** (문자열): 수정일시. yyyy-MM-dd HH:mm:ssZ 형식
* **closed** (문자열): 완료일시. yyyy-MM-dd HH:mm:ssZ 형식
* **x\_login** (문자열): 티켓 작성 계정 삭제 시 기록되는 로그인 계정 이름
* **x\_user** (문자열): 티켓 작성 계정 삭제 시 기록되는 사용자 성명
* **x\_dept** (문자열): 티켓 작성 계정 삭제 시 기록되는 부서 이름
* **x\_site** (문자열): 사이트 삭제 시 기록되는 사이트 이름
* **comments** (배열): 티켓 메모 목록
* **guid** (문자열): 티켓 메모 식별자
* **user\_guid** (문자열): 티켓 작성자 식별자
* **user\_name** (문자열): 티켓 작성자 성명
* **type** (문자열): TEXT 고정.
* **format** (문자열): 마크다운 (MARKDOWN), 일반 텍스트 (PLAIN) 중 하나.
* **content** (문자열): 메모 내용
* **created** (문자열): 생성일시. yyyy-MM-dd HH:mm:ssZ 형식
* **updated** (문자열): 수정일시. yyyy-MM-dd HH:mm:ssZ 형식
* **x\_login** (문자열): 메모 작성 계정 삭제 시 기록되는 로그인 계정 이름
* **x\_user** (문자열): 메모 작성 계정 삭제 시 기록되는 사용자 성명
* **x\_dept** (문자열): 메모 작성 계정 삭제 시 기록되는 부서 이름

#### 오류 응답

티켓이 존재하지 않는 경우

HTTP 상태 코드 200 응답

{ "ticket": null}

티켓 식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

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