### 로그 스키마 조회

지정한 로그 스키마의 필드 구성 정보를 조회합니다.

#### HTTP 요청

GET /api/sonar/log-schemas/:code

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/log-schemas/session

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| code | O | 문자열 | 로그 스키마 코드 |  |

#### 정상 응답

아래는 session 로그 스키마에 대한 조회 예시입니다.

{ "schema": { "code": "session", "name": "세션", "description": "방화벽 세션 및 네트워크 플로우", "created": "2022-09-01 00:31:13+0900", "fields": [ { "name": "\_time", "display\_name": "시각", "type": "DATE", "ordinal": 1 }, { "name": "src\_ip", "display\_name": "출발지IP", "type": "IP", "ordinal": 2 }, { "name": "src\_port", "display\_name": "출발지포트", "type": "PORT", "ordinal": 3 }, { "name": "dst\_ip", "display\_name": "목적지IP", "type": "IP", "ordinal": 4 }, { "name": "dst\_port", "display\_name": "목적지포트", "type": "PORT", "ordinal": 5 }, { "name": "protocol", "display\_name": "프로토콜", "type": "STRING", "ordinal": 6 }, { "name": "app", "display\_name": "응용", "type": "STRING", "ordinal": 7 }, { "name": "action", "display\_name": "대응", "type": "STRING", "ordinal": 8 }, { "name": "nat\_src\_ip", "display\_name": "NAT출발지IP", "type": "IP", "ordinal": 9 }, { "name": "nat\_src\_port", "display\_name": "NAT출발지포트", "type": "PORT", "ordinal": 10 }, { "name": "nat\_dst\_ip", "display\_name": "NAT목적지IP", "type": "IP", "ordinal": 11 }, { "name": "nat\_dst\_port", "display\_name": "NAT목적지포트", "type": "PORT", "ordinal": 12 }, { "name": "policy", "display\_name": "정책", "type": "STRING", "ordinal": 13 }, { "name": "duration", "display\_name": "접속시간", "type": "LONG", "ordinal": 14 }, { "name": "total\_bytes", "display\_name": "바이트", "type": "STRING", "ordinal": 15 }, { "name": "total\_pkts", "display\_name": "패킷", "type": "STRING", "ordinal": 16 }, { "name": "sent\_pkts", "display\_name": "송신패킷", "type": "LONG", "ordinal": 17 }, { "name": "rcvd\_pkts", "display\_name": "수신패킷", "type": "LONG", "ordinal": 18 }, { "name": "sent\_bytes", "display\_name": "송신바이트", "type": "LONG", "ordinal": 19 }, { "name": "rcvd\_bytes", "display\_name": "수신바이트", "type": "LONG", "ordinal": 20 }, { "name": "src\_country", "display\_name": "출발지국가", "type": "COUNTRY", "ordinal": 21 }, { "name": "dst\_country", "display\_name": "목적지국가", "type": "COUNTRY", "ordinal": 22 } ] }}

* **schema** (맵): 로그 스키마 정의
* **code** (문자열): 코드
* **name** (문자열): 이름
* **description** (문자열): 설명
* **created** (문자열): 생성일시 (yyyy-MM-dd HH:mm:ssZ 형식)
* **fields** (배열): 정규화된 필드 정의 목록
* **name** (문자열): 필드 이름
* **display\_name** (문자열): 화면 표시 이름
* **type** (문자열): 유형. DATE, STRING, IP, PORT, INT, LONG, DOUBLE, COUNTRY, MD5, SHA1, URL 중 하나.
* **ordinal** (32비트 정수): 필드 표시 순서

#### 오류 응답

로그 스키마가 존재하지 않는 경우

HTTP 상태 코드 200 응답

{ "schema": null}