### 실시간 탐지 명령어 템플릿 목록 조회

모든 실시간 탐지 명령어 템플릿 목록을 조회합니다.

실시간 탐지 명령어 템플릿은 GUI 방식의 실시간 탐지 시나리오 편집을 지원하는 용도로 사용합니다.

#### HTTP 요청

GET /api/sonar/stream-rule-command-templates

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/stream-rule-command-templates

#### 정상 응답

아래는 전체 실시간 탐지 명령어 템플릿 목록 중 일부입니다.

{ "templates": [ { "id": 2, "name": "IP 주소 일치", "field\_type": "IP", "description": null, "config\_specs": [ { "name": "ip", "type": "string", "subtype": "ip", "display\_name": "비교 IP", "description": "비교 대상 IP를 입력합니다." } ], "query": "search $field$ == ip($ip$)", "query2": "search $field$ != ip($ip$)" }, { "id": 3, "name": "IP 주소가 네트워크 대역에 포함", "field\_type": "IP", "description": null, "config\_specs": [ { "name": "subnet", "type": "string", "subtype": "subnet", "display\_name": "비교 네트워크 대역", "description": "비교 대상 네트워크 그룹을 선택합니다." } ], "query": "matchnet field=$field$ guid=$subnet$ verify=f", "query2": "matchnet invert=t field=$field$ guid=$subnet$ verify=f" } ]}

* **templates** (배열): 모든 실시간 탐지 명령어 템플릿 목록
* **id** (32비트 정수): 템플릿 고유 식별자
* **name** (문자열): 템플릿 이름
* **field\_type** (문자열): 적용 대상 필드 유형. DATE, IP, PORT, STRING, SHORT, INT, LONG, MD5, URL 중 하나.
* **description** (문자열): 템플릿 설명
* **config\_specs** (배열): 템플릿 변수 명세 목록
* **name** (문자열): 변수 이름
* **type** (문자열): 변수 타입. string, number, array
* **subtype** (문자열): UI 렌더링 힌트. ip, date, country, port\_group 등 자동완성 및 유효성 검사를 지원하는 컴포넌트 선택을 지원하는 용도.
* **display\_name** (문자열): 로케일 적용된 변수 이름
* **description** (문자열): 로케일 적용된 변수 설명
* **query** (문자열): AND 조건에서 적용할 쿼리 문자열
* **query2** (문자열): NOT 조건에서 적용할 쿼리 문자열