### 배치 탐지 시나리오 목록 조회

검색 조건과 일치하는 배치 탐지 시나리오 목록을 조회합니다.

#### HTTP 요청

GET /api/sonar/batch-rules

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/batch-rules

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| offset | X | 32비트 정수 | 건너뛸 갯수 | 기본값 0 |
| limit | X | 32비트 정수 | 최대 갯수 | 미지정 시 전체 조회 |
| keywords | X | 문자열 | 검색 키워드 | 이름, 설명, 쿼리 대상으로 검색 |
| category\_guids | X | 문자열 목록 | 시나리오 분류 GUID 목록 | 쉼표(,)를 구분자로 하는 GUID 목록 |
| enabled | X | 불리언 | 탐지 활성화 여부 |  |
| use\_ticket | X | 불리언 | 티켓 사용 여부 |  |
| use\_explanation | X | 불리언 | 소명 사용 여부 |  |

#### 정상 응답

아래는 배치 탐지 시나리오 목록 중 일부입니다.

{ "total\_count": 1, "rules": [ { "guid": "f4ca02c8-0679-49e7-8c10-76667c26b595", "priority": "LOW", "name": "DMZ 포트 스캔", "description": "", "msg": "DMZ 포트 스캔: $src\_ip", "enabled": false, "category\_guid": "8270a382-a47c-401d-9318-037c5d639f2e", "category\_name": "정보 수집", "schedule": "\*/10 \* \* \* \*", "duration": null, "datetrunc": null, "dataset\_guid": null, "dataset\_name": null, "query": "table duration=30m FW\_\*\n| fields \_time, \_schema, src\_ip, src\_port, dst\_ip, dst\_port, protocol, app, action, sent\_pkts, rcvd\_pkts, sent\_bytes, rcvd\_bytes\n| search \_schema == \"session\" and protocol == \"TCP\" and sent\_bytes <= 200\n| lookup geoip src\_ip output country as src\_country\n| lookup geoip dst\_ip output country as dst\_country\n| search src\_country != \"--\"\n| eval \_time = datetrunc(\_time, \"10m\") \n| stats dc(dst\_port) as port\_count, values(dst\_port) as dst\_port by src\_ip, dst\_ip, \_time \n| search port\_count >= 10 \n| explode dst\_port \n| eval protocol = \"TCP\" \n| order \_time, host\_count, src\_ip, dst\_ip, dst\_port, protocol", "address\_group\_guid": null, "address\_field": null, "ticket\_repo\_guid": null, "ticket\_assignee\_guid": null, "ticket\_assignee\_name": null, "ticket\_suppress\_interval": 3600, "event\_suppress\_interval": 0, "suppress\_key": null, "keep\_alive": false, "audit\_category\_guid": null, "audit\_category\_name": null, "auditor\_guid": null, "auditor\_name": null, "audit\_days": 14, "employee\_key\_field": null, "alarm\_group\_guid": null, "alarm\_group\_name": null, "field\_order": "\_time, host\_count, src\_ip, dst\_ip, dst\_port, protocol", "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": null, "user\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "user\_name": "관리자", "created": "2022-09-01 00:31:15+0900", "updated": "2022-09-01 00:31:15+0900" } ]}

* **total\_count** (32비트 정수): 검색 조건과 일치하는 전체 배치 탐지 시나리오 갯수
* **rules** (배열): 페이징된 배치 탐지 시나리오 목록
* **priority** (문자열): LOW, MEDIUM, HIGH 중 하나.
* **guid** (문자열): 배치 탐지 시나리오 GUID
* **name** (문자열): 배치 탐지 시나리오 이름
* **description** (문자열): 배치 탐지 시나리오 설명
* **msg** (문자열): 메시지 템플릿. $field 형식의 매크로를 사용하여 필드 값을 메시지에 반영할 수 있음.
* **enabled** (불리언): 탐지 활성화 여부
* **category\_guid** (문자열): 탐지 시나리오 분류 GUID
* **category\_name** (문자열): 탐지 시나리오 분류 이름
* **schedule** (문자열): 실행 주기. CRON 일정 문법 사용
* **duration** (32비트 정수): 분석 대상 기간 (초). 설정 값은 쿼리의 from, to 매개변수로 전달됩니다.
* **datetrunc** (32비트 정수): 시간 절사 단위 (초). from, to 쿼리 매개변수의 시간 절사.
* **dataset\_guid** (문자열): 데이터셋 GUID
* **dataset\_name** (문자열): 데이터셋 이름
* **address\_group\_guid** (문자열): 주소 그룹 GUID
* **address\_field** (문자열): 주소 그룹에 등록할 대상 필드
* **ticket\_repo\_guid** (문자열): 티켓 분류 GUID
* **ticket\_assignee\_guid** (문자열): 티켓 할당자 GUID
* **ticket\_assignee\_name** (문자열): 티켓 할당자 성명
* **ticket\_suppress\_interval** (32비트 정수): 중복 티켓 축약 기간 (초 단위)
* **event\_suppress\_interval** (32비트 정수): 중복 이벤트 제거 기간 (초 단위)
* **suppress\_key** (문자열): 중복 기준 필드. $field 형식으로 지정된 매크로를 해당 필드 값으로 대체하여 이벤트 컨텍스트 키로 사용함.
* **keep\_alive** (불리언): true인 경우 축약 타이머 유지. false인 경우 축약 타이머 초기화.
* 축약 타이머 유지 시 티켓을 완료 처리하더라도 만료 시간에 도달할 때까지 이벤트가 기존 티켓에 병합됩니다.
* **audit\_category\_guid** (문자열): 소명 분류 GUID
* **audit\_category\_name** (문자열): 소명 분류 이름
* **auditor\_guid** (문자열): 소명 확인 계정의 GUID. 미지정 시 부서장 전결.
* **auditor\_name** (문자열): 소명 확인 계정의 성명. 미지정 시 부서장 전결.
* **audit\_days** (32비트 정수): 소명 제출 마감 시한 (일 단위)
* **employee\_key\_field** (문자열): 사번 필드 이름. 통상 정규화된 필드인 emp\_key를 사용함.
* **alarm\_group\_guid** (문자열): 알람 그룹 GUID
* **alarm\_group\_name** (문자열): 알람 그룹 이름
* **field\_order** (문자열): 근거 자료 출력 시 필드 순서. 쉼표로 구분된 필드 이름 목록.
* **company\_guid** (문자열): 시나리오가 속한 회사 (테넌트) GUID
* **company\_name** (문자열): 시나리오가 속한 회사 (테넌트) 이름
* **user\_guid** (문자열): 시나리오를 생성한 사용자 GUID
* **user\_name** (문자열): 시나리오를 생성한 사용자 성명
* **created** (문자열): 생성일시 (yyyy-MM-dd HH:mm:ssZ 형식)
* **updated** (문자열): 수정일시 (yyyy-MM-dd HH:mm:ssZ 형식)

#### 오류 응답

offset, limit 값이 정수가 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset, limit 값이 음수인 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

시나리오 분류 식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

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