### 실시간 탐지 시나리오 생성

새 실시간 탐지 시나리오를 생성합니다.

#### HTTP 요청

POST /api/sonar/stream-rules

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d priority="HIGH" \ -d name="알려진 봇넷 대역 접속" \ -d msg="알려진 봇넷 대역 접속: $dst\_ip" \ -d schema\_code="session" \ -d commands="[{'template\_id': 3, 'query': 'matchnet invert=t field=dst\_ip guid=697393b6-aecf-4e9d-a32c-8724cd8f067e verify=f', 'field\_name': 'dst\_ip', 'args':{'subnet':'697393b6-aecf-4e9d-a32c-8724cd8f067e'}}]" \ -X POST \ https://HOSTNAME/api/sonar/stream-rules

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| priority | O | 문자열 | 중요도 | LOW, MEDIUM, HIGH 중 하나 |
| guid | X | 문자열 | 실시간 탐지 시나리오 GUID | 36자 |
| name | O | 문자열 | 실시간 탐지 시나리오 이름 | 최소 1자, 최대 255자 |
| description | X | 문자열 | 실시간 탐지 시나리오 설명 | 최대 2,000자 |
| msg | O | 문자열 | 메시지 템플릿 | 최소 1자, 최대 2,000자 |
| enabled | X | 불리언 | 활성화 여부 | true 혹은 false |
| category\_guid | X | 문자열 | 시나리오 분류 GUID | 36자 |
| schema\_code | O | 문자열 | 정규화 스키마 식별자 | 최소 1자, 최대 50자 |
| logger\_guids | O | 배열 | 수집기 GUID 목록 |  |
| commands | O | 배열 | 실시간 탐지 명령어 목록 | 1개 이상의 명령어 필요. 하단 설명 참조 |
| address\_group\_guid | X | 문자열 | 주소 그룹 GUID | 36자 |
| address\_field | X | 문자열 | 주소 필드 | 주소 그룹에 등록할 필드 이름. 최대 50자 |
| ticket\_repo\_guid | X | 문자열 | 티켓 분류 GUID | 미설정 시 티켓 발생하지 않음. 36자 |
| ticket\_assignee\_guid | X | 문자열 | 티켓 할당자 GUID | 지정 시 담당자 자동 할당 |
| ticket\_suppress\_interval | X | 32비트 정수 | 중복 티켓 축약 기간 | 초 단위. 0 또는 미설정 시 동일 티켓을 병합하지 않음 |
| event\_suppress\_interval | X | 32비트 정수 | 중복 이벤트 제거 기간 | 초 단위. 0 또는 미설정 시 중복 이벤트를 제거하지 않음 |
| suppress\_key | X | 문자열 | 중복 기준 필드 | $field 형식으로 매크로 사용 가능. 최대 2,000자 |
| keep\_alive | X | 불리언 | 축약 타이머 유지 여부 | 축약 타이머 유지 시 true, 초기화 시 false |
| audit\_category\_guid | X | 문자열 | 소명 분류 GUID | 미설정 시 자동 소명 요청이 비활성화됨. 36자 |
| auditor\_guid | X | 문자열 | 소명 확인 계정 GUID | 미설정 시 부서장 전결. 36자 |
| audit\_days | X | 32비트 정수 | 소명 제출 마감 시한 | 최소 1일, 최대 365일 |
| employee\_key\_field | X | 문자열 | 사번 필드 이름 | 미설정 시 자동 소명 요청이 비활성화됨. 최대 50자 |
| alarm\_group\_guid | X | 문자열 | 알람 그룹 GUID | 36자 |
| field\_order | X | 문자열 | 근거 자료 필드 출력 순서 | 최대 2,000자 |

commands의 각 배열 요소는 아래와 같이 정의합니다:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| template\_id | O | 32비트 정수 | 실시간 탐지 명령어 템플릿 ID |  |
| query | O | 문자열 | 부분 쿼리 문자열 |  |
| field\_name | X | 문자열 | 대상 필드 이름 |  |
| args | X | 맵 | 인자 키/값 |  |
| invert | X | 불리언 | 반전 여부 |  |

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "schema\_code should be not null"}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'schema\_code' must be shorter than or equal to 50 characters."}

잘못된 중요도 값을 사용한 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "priority should be one of 'LOW', 'MEDIUM', 'HIGH'."}

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

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

실시간 탐지 명령어 목록이 유효한 JSON 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'commands' parameter should follow valid JSON syntax"}

정규화 스키마가 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "schema not found: unknown"}

시나리오 생성 권한이 없는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}