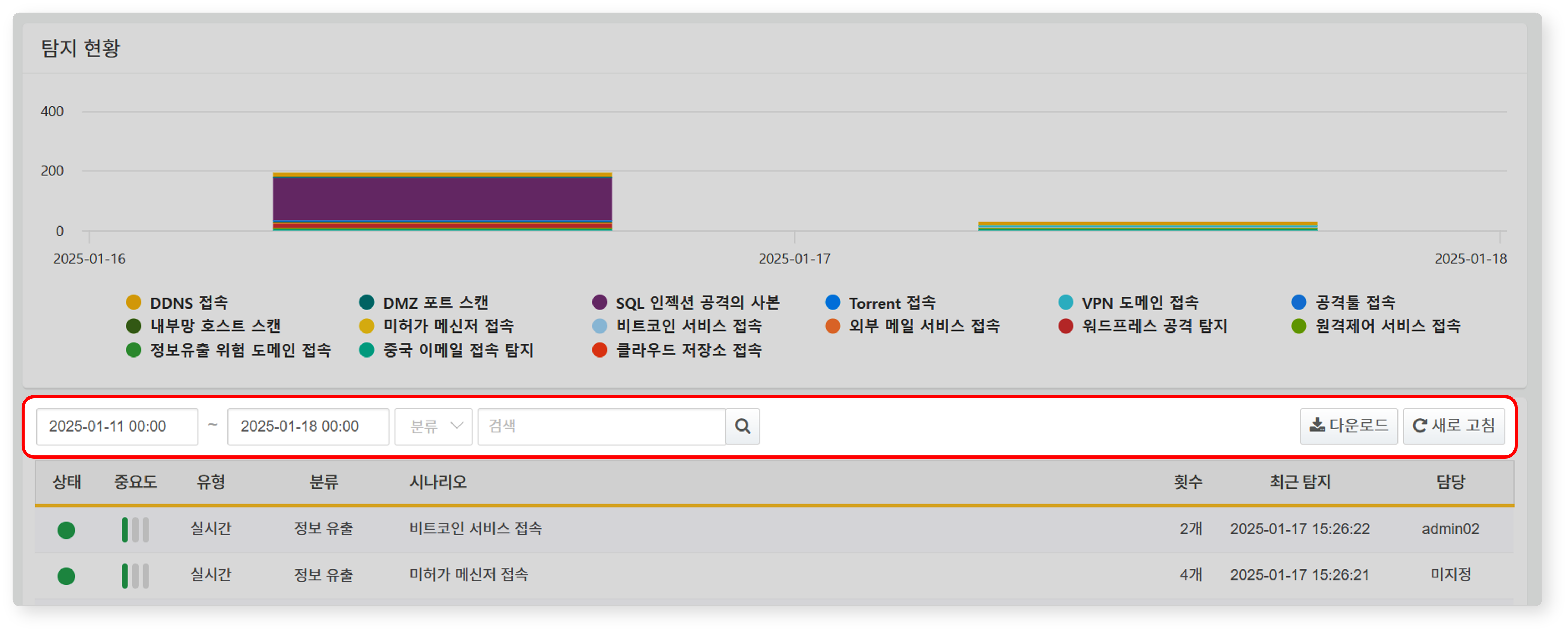
### 탐지 현황

#### 개요

**분석 > 탐지 현황**에서 시나리오별로 이벤트 탐지 현황을 시각적으로 제공합니다. 탐지 현황은 시나리오에 따라 탐지된 이벤트의 발생 횟수를 보여주는 차트와 목록으로 구성되어 있습니다. 기간을 지정하거나, 이벤트 분류, 검색어를 조회 조건으로 지정할 수 있습니다.

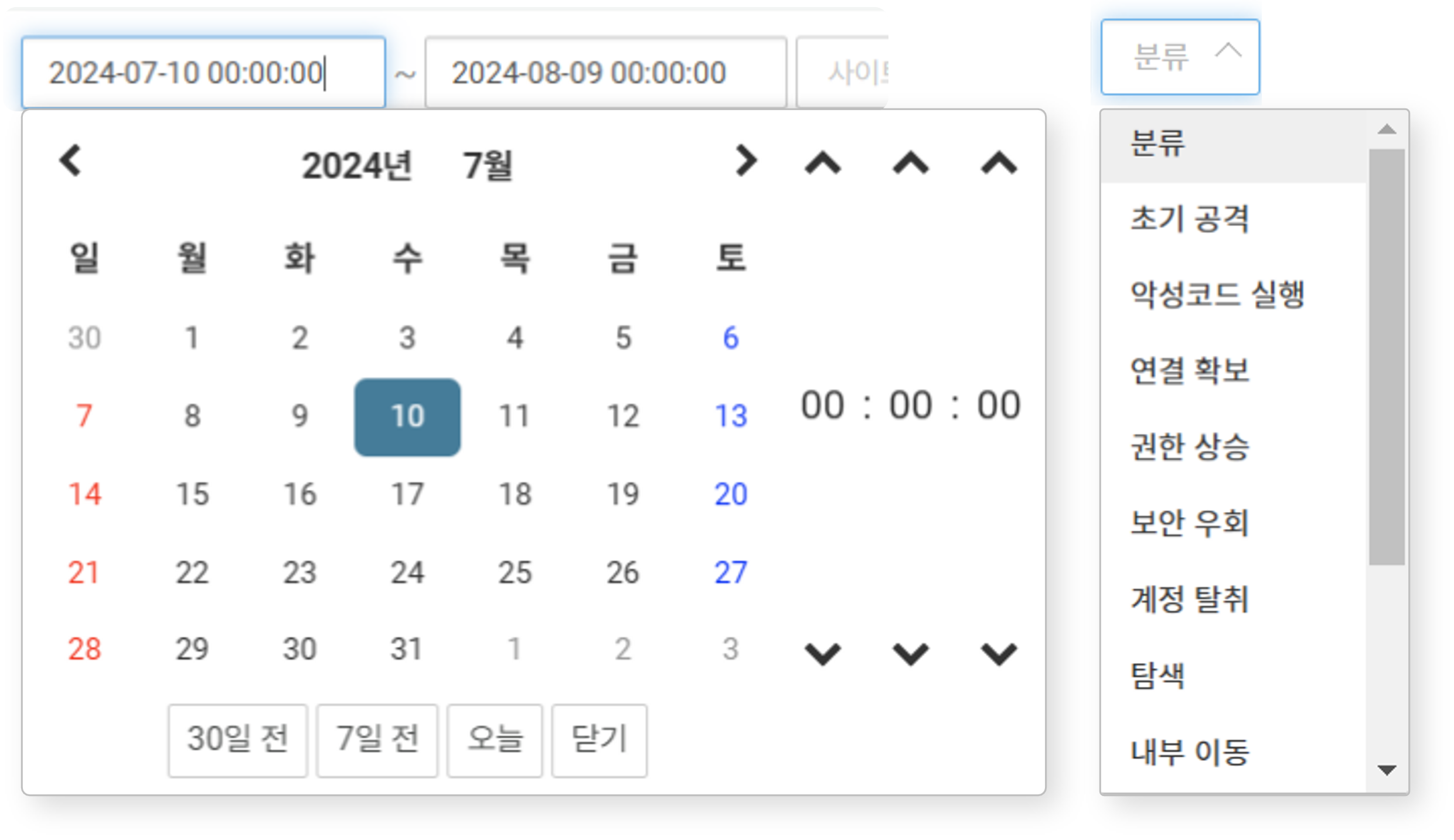
#### 도구 모음

[탐지 현황 목록](https://docs.logpresso.com/ko/sonar/4.0/ui/section-event-summary) 위에는 탐지 현황을 필터링하거나 검색하여 볼 수 있도록 도구 모음을 제공합니다. 필터와 검색 조건을 지정하면 그에 맞춰 탐지 현황 차트와 목록이 갱신됩니다. 그 외에 탐지 현황 목록 다운로드, 탐지 현황 목록 새로 고침 기능을 제공합니다.



기간/분류 필터

탐지 현황을 검색할 기간과 이벤트 분류를 지정하면 해당 조건에 맞도록 차트와 목록을 갱신합니다. 다음 그림은 탐지 이벤트가 발생한 **기간**, 탐지 현황 **분류** 필터의 예시입니다.



도구 모음에서 사용할 수 있는 필터는 다음과 같습니다.

* **기간**: 이벤트를 조회할 기간을 선택(기본값: 조회 시점 기준으로 당일 0시 ~ 익일 0시. 익일 0시는 검색 범위에 포함되지 않습니다). 도구 모음에서 입력 상자에 직접 입력하거나, 입력 상자를 클릭했을 때 나타나는 시간 선택기를 통해 기간을 지정할 수 있습니다.
* **분류**: 조회할 이벤트 분류 선택(기본값: 전체 선택). 이벤트의 분류는 탐지 시나리오에 지정된 분류를 따릅니다. 분류는 **정책 > 실시간 탐지 또는 배치 탐지**의 [시나리오 분류 관리](https://docs.logpresso.com/ko/sonar/4.0/ui/section-stream-rule)에서 관리할 수 있습니다.

검색 필터

탐지 현황 목록에서 특정한 탐지 현황을 찾으려면 도구 모음에 있는 검색 도구를 사용하세요. 검색 도구는 **시나리오**에서 검색어가 포함된 탐지 현황을 찾아서 보여줍니다. 탐지 현황 검색 도구는 대소문자를 구분하지 않습니다.



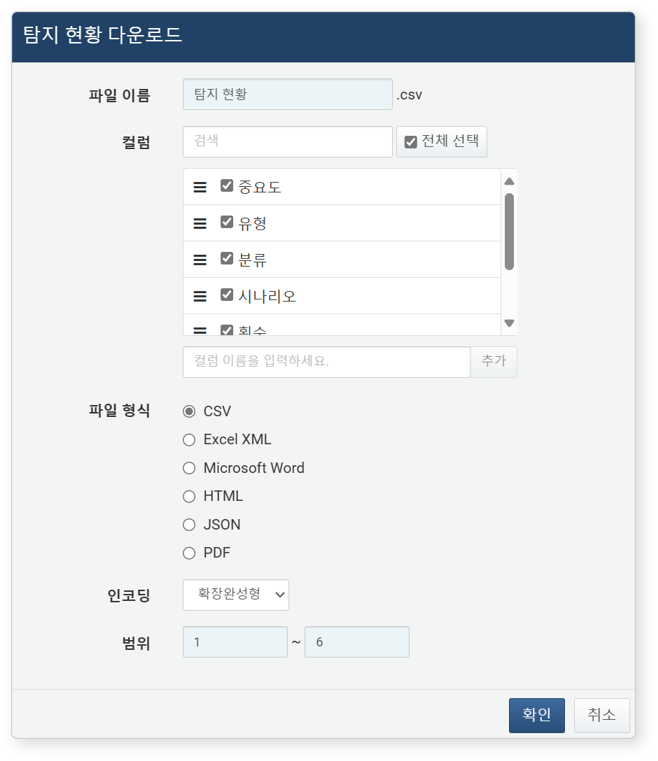
효과적인 검색을 위해 기간/분류 필터를 함께 사용하세요. 기간 필터는 항상 검색에 적용됩니다.

다운로드

조회 중인 [탐지 현황 목록](https://docs.logpresso.com/ko/sonar/4.0/ui/section-event-summary)을 다운로드하려면,

도구 모음에서 **다운로드**를 클릭하세요.

**탐지 현황 다운로드** 창에서 다음 속성을 입력하거나 선택한 다음, **확인**을 클릭하세요.



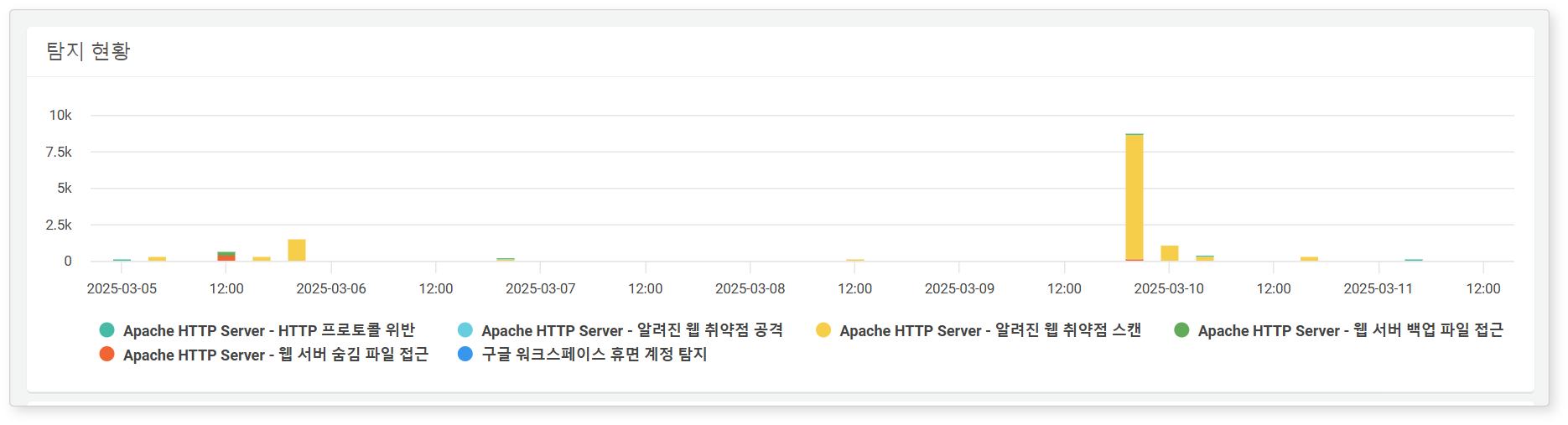
* **파일 이름**: 다운로드할 탐지 현황 목록 파일의 이름(기본값: 티켓)
* **컬럼**: 파일에 저장할 탐지 현황 속성. **전체 선택**을 클릭하면 모든 속성을 파일에 기록합니다.
* **파일 형식**: 다운로드할 파일의 형식(기본값: CSV)
* **CSV**: CSV 파일
* **Excel XML**: Microsoft Excel에서 열어볼 수 있는 XML 파일
* **Microsoft Word**: DOCX 파일
* **HTML**: HTML 파일
* **JSON**: JSON 파일
* **PDF**: PDF 파일
* **파일 인코딩**: 파일 인코딩(UTF-8, UTF-18 BE, 확장완성형, 기본값: 확장완성형)
* **범위**: 파일에 기록할 탐지 현황 개수. 최근에 등록된 탐지 현황부터 역순으로 지정된 개수만큼만 파일에 기록합니다.

새로 고침

탐지 현황 목록을 최신 정보로 조회하려면 도구 모음에서 **새로 고침**을 클릭하세요.

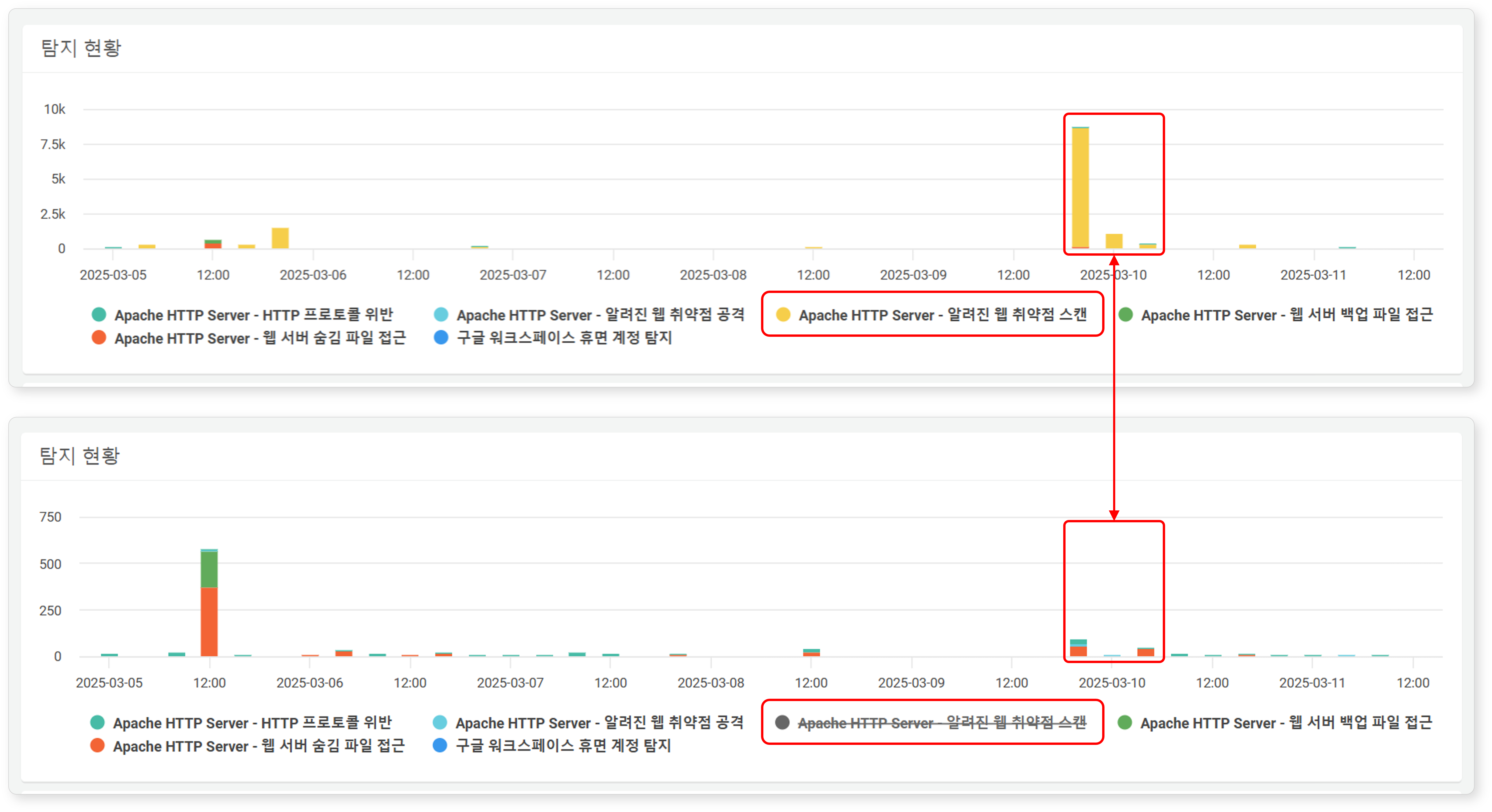
#### 탐지 현황 차트

탐지 현황 차트는 시나리오별로 최근 7일 간 탐지 횟수를 보여줍니다(X 축: 시간, Y 축: 탐지 횟수).



시나리오 필터

차트 하단에 시나리오 범례가 있습니다. 범례에서 특정 시나리오를 클릭하면 차트에서 해당 시나리오의 탐지 현황을 숨기거나 표시합니다.



기간 필터

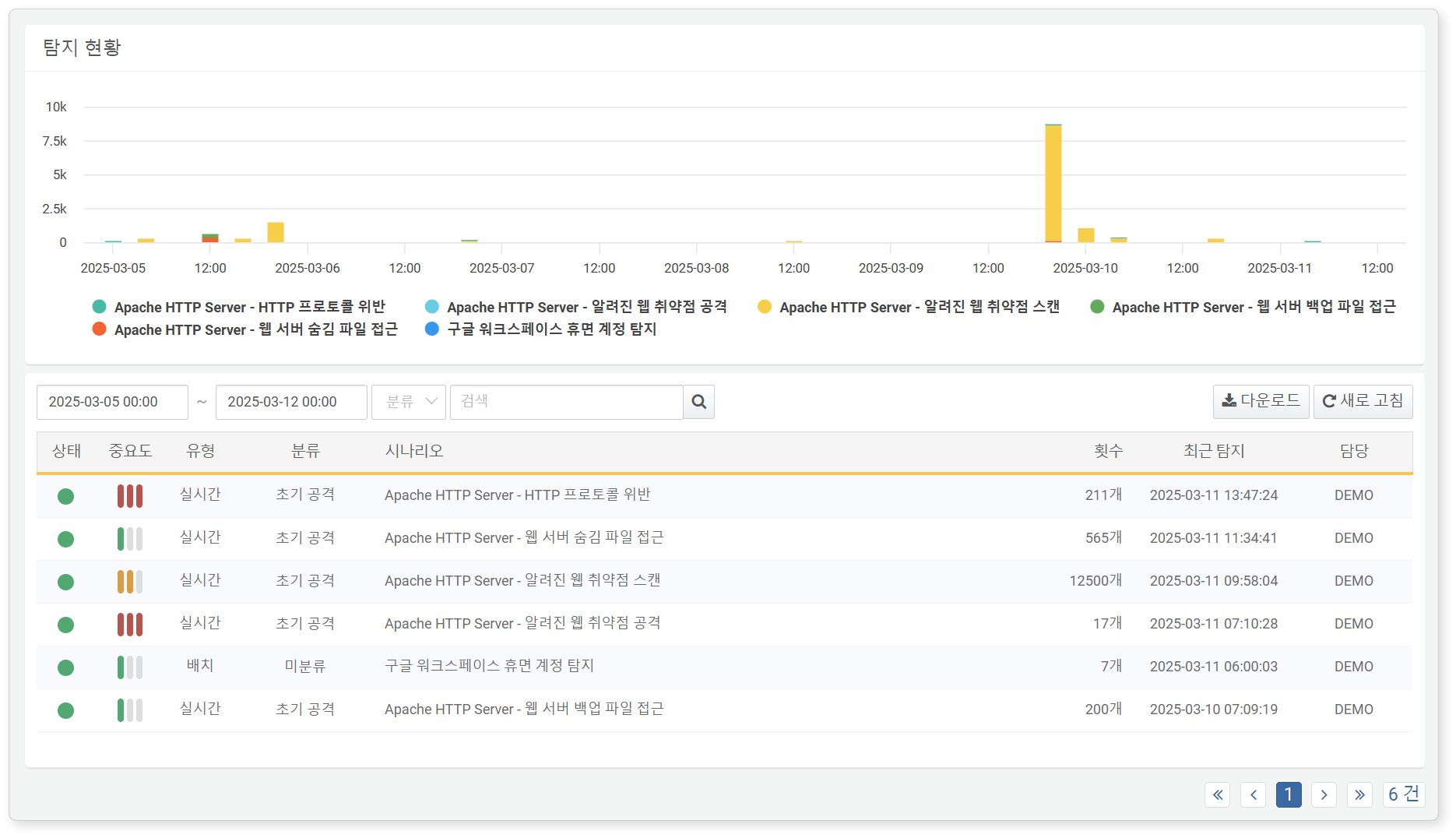
차트 위에 마우스 포인터를 이동시킨 후 드래그 & 드롭하면 드래그 한 구간에 한정해서 이벤트 현황을 조회할 수 있습니다.



차트에서 **RESET**을 클릭하면 이벤트 기간 필터가 해제됩니다.

#### 탐지 현황 목록

탐지 현황 목록은 시나리오를 기준으로 최근 7일 간 발생한 이벤트의 분류, 발생 횟수, 중요도 등을 최근 탐지 시각을 기준으로 보여줍니다. 이벤트가 탐지되지 않은 시나리오는 목록에서 보여주지 않습니다.



탐지 현황 목록에서 확인할 수 있는 정보는 다음과 같습니다.

* **상태**: 탐지 시나리오 정책의 상태(**초록색**: 활성화, **회색**: 비활성화)
* **중요도**: 탐지 시나리오 정책에 따른 이벤트 중요도 (상/중/하)
* **유형**: 탐지 시나리오의 유형 (실시간/배치)
* **분류**: 시나리오에 의해 이벤트에 적용된 분류 정보
* **시나리오**: 이벤트를 탐지한 시나리오의 이름
* **횟수**: 이벤트 발생 횟수
* **최근 탐지**: 최근에 탐지된 이벤트의 발생 시각
* **담당**: 탐지된 이벤트에 대해 발행된 [티켓](https://docs.logpresso.com/ko/sonar/4.0/ui/section-ticket)을 처리할 담당자. 담당자가 할당되어 있지 않으면 **미지정**으로 표시됩니다.

탐지 현황 목록은 이벤트를 탐지한 시나리오를 기준으로 합니다. 탐지 시나리오를 수정하면 수정된 시나리오에 따라 탐지 현황이 갱신됩니다. 단, 탐지 시나리오의 이름을 변경하면 기존 이벤트는 탐지 현황 목록에서 사라지고, 변경된 이름의 시나리오에 따라 탐지된 이벤트만 보여줍니다.

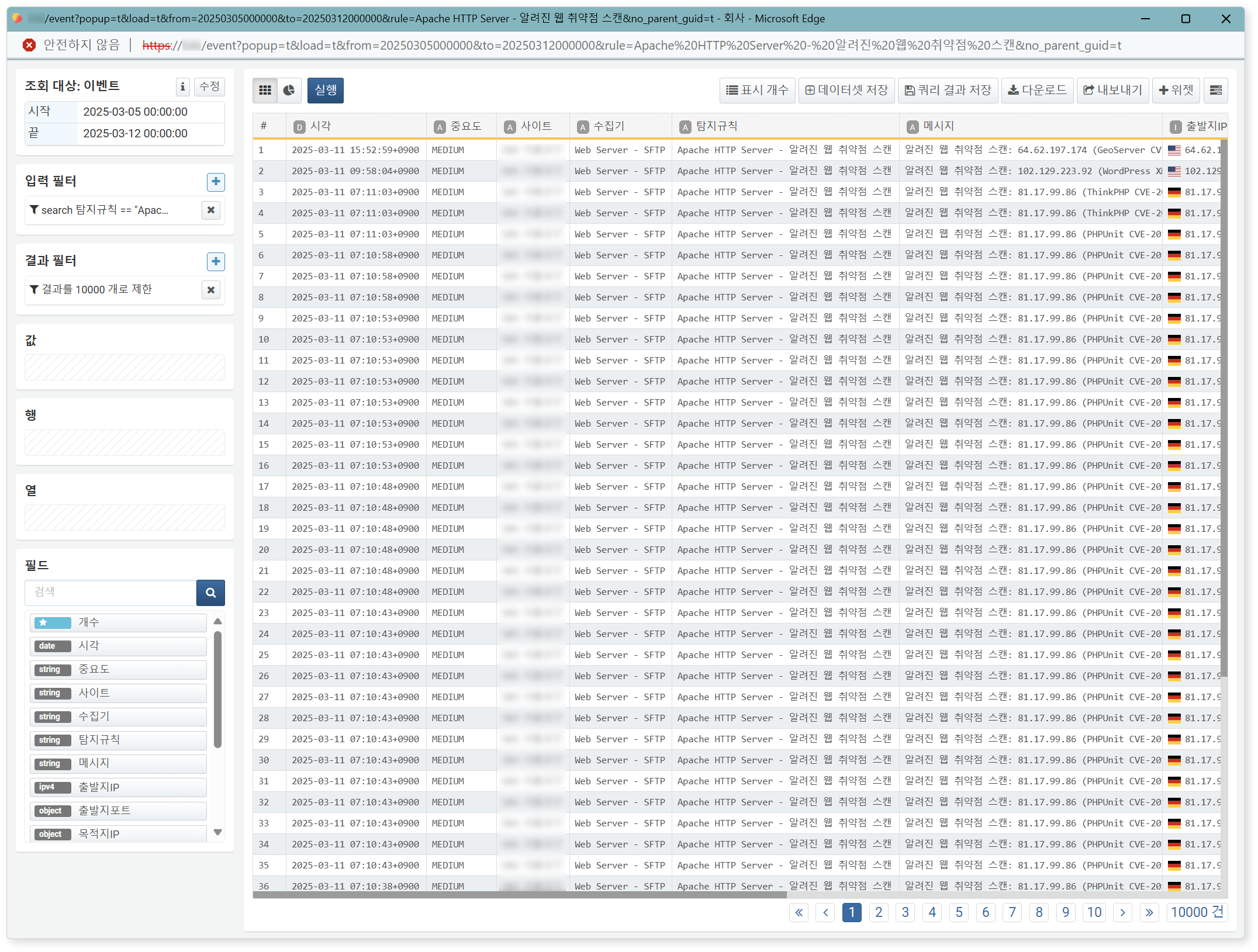
#### 시나리오별 현황 상세 조회

이벤트의 상세 내역을 조회하려면,

[탐지 현황 목록](https://docs.logpresso.com/ko/sonar/4.0/ui/section-event-summary)에서 조회할 이벤트 탐지 시나리오의 이름을 클릭하세요.

팝업 창에서 이벤트 탐지 시나리오별 탐지된 이벤트에 대한 상세 내역을 조회할 수 있습니다.

✅ 이벤트 상세 내역 화면에서 수행할 수 있는 작업들은 [이벤트](https://docs.logpresso.com/ko/sonar/4.0/ui/section-events)에서 수행할 수 있는 작업과 동일합니다.



이 화면에서 보여주는 이벤트 정보는 원본 데이터를 정규화한 것입니다. 티켓의 근거자료에서 보여주는 이벤트 정보는 정규화되지 않은 원본을 보여줍니다.