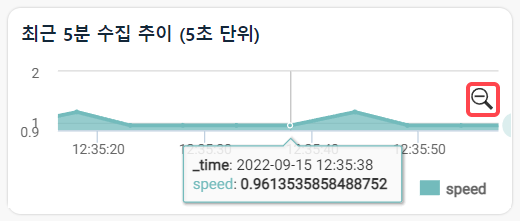
#### 이벤트 동작

클릭이나 드래그 이벤트가 발생했을 때 위젯이 실행할 수 있는 동작은 줌인/줌아웃, 쿼리 실행, 필터링, 브라우저 실행, 백그라운드 쿼리 실행이 있습니다.

줌인/줌아웃

줌인/줌아웃은 드래그 이벤트의 기본 동작으로, 독립 변수와 종속 변수로 구성되는 차트(예: 모든 막대 차트, 라인 차트, 산포도 차트, 버블 차트, 박스플롯 차트, 영역 차트)에서 차트의 일부분을 드래그하면 해당 부분을 확대해서 볼 수 있습니다. 위젯 새로고침 주기가 되거나 줌아웃 버튼을 누르면 다시 원상태로 돌아갑니다.

줌인/줌아웃은 이벤트가 발생한 위젯에서만 동작하고, 다른 위젯에 영향을 주지 않습니다.



브라우저 실행

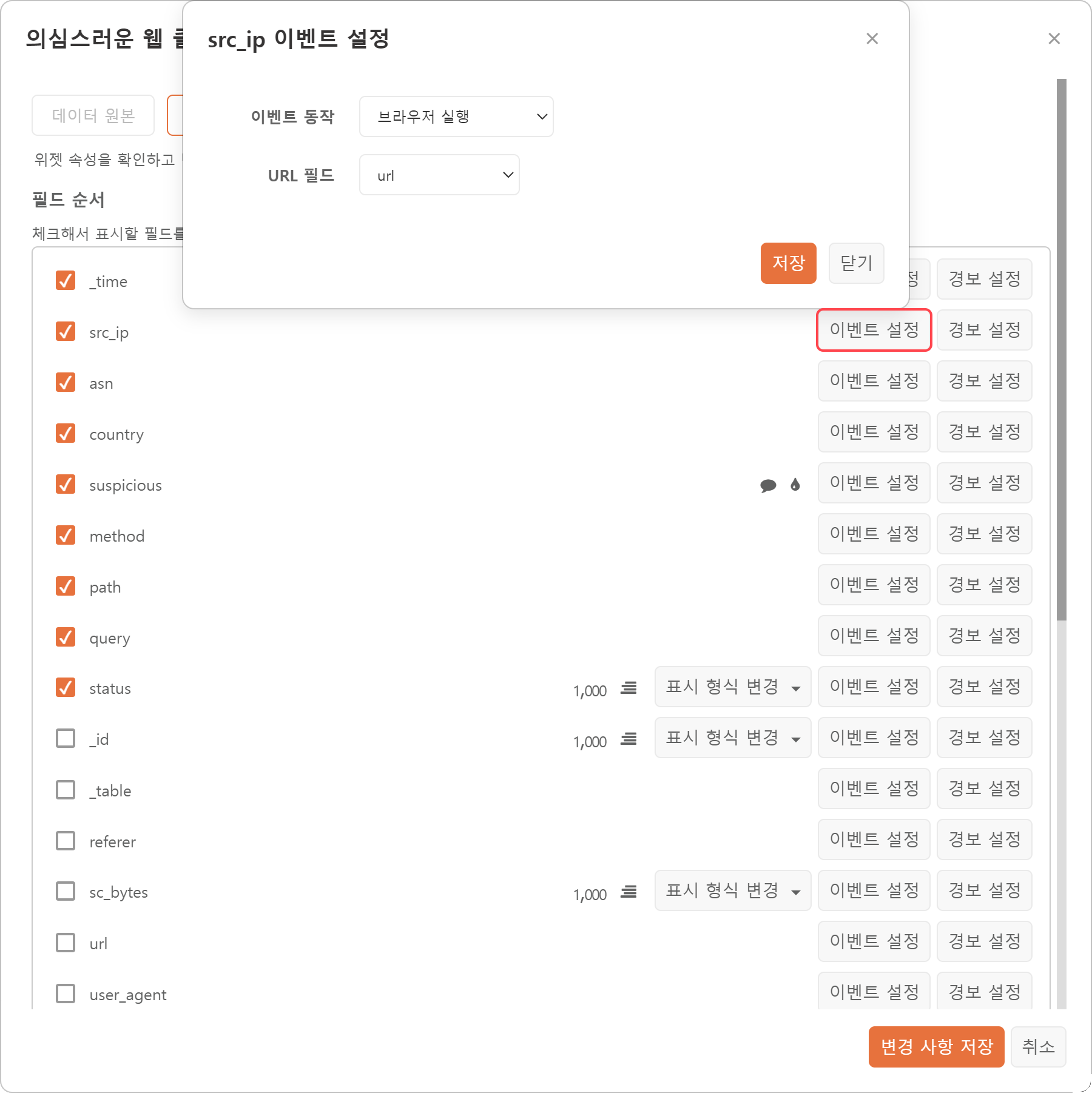
브라우저 실행은 클릭 이벤트가 발생했을 때 url 정보를 가진 필드의 값을 인자로 받은 후 웹 브라우저로 연결하는 기능입니다.

이 동작을 사용하려면 위젯이 가져온 데이터에 url 정보가 포함된 필드가 있어야 합니다.

예제

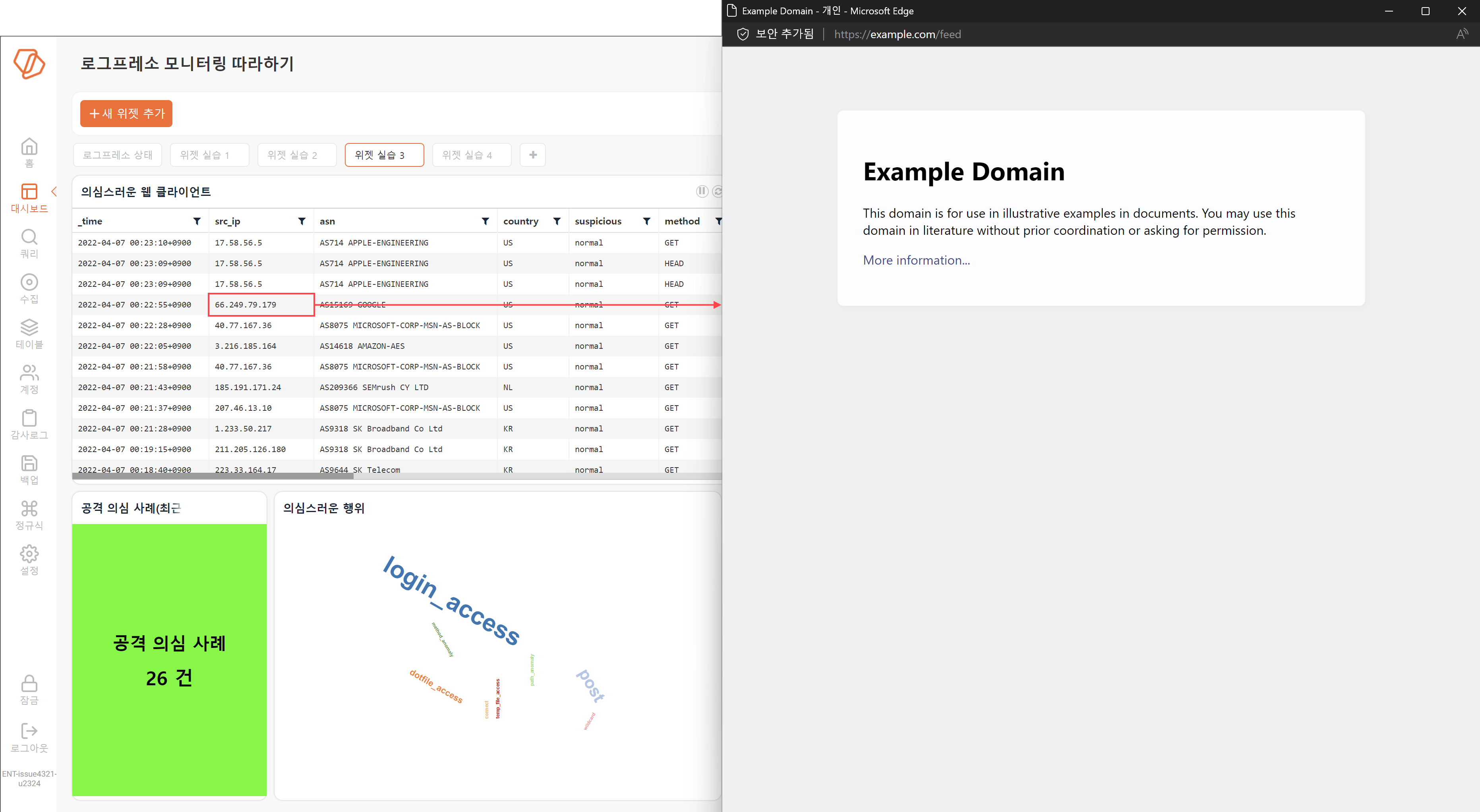
이 예제의 목표는 그리드 위젯에서 사용자가 **src** 필드를 누르면 해당 출발지 IP 주소에서 접속한 URL을 브라우저로 열어볼 수 있게 하는 것입니다.

[그리드 위젯 예제](https://docs.logpresso.com/ko/enterprise/4.0/ui/data-widget-grid)를 참고하여 위젯을 추가합니다. 위젯을 설정할 때 다음과 같이 이벤트 속성을 지정합니다.



* **필드 순서**에서 **src\_ip** 필드를 선택하고 **이벤트 설정**을 누릅니다.
* **이벤트 동작**: 브라우저 실행
* **URL 필드**: url

그리드 위젯에서 **src\_ip** 필드값이 66.249.79.179인 셀을 누르고, 웹 브라우저가 **url** 필드로 지정된 주소로 접근하는지 확인합니다.



**쿼리 > 쿼리**에서 다음 쿼리를 실행해보고 실제로 웹 브라우저가 접근한 URL이 맞는지 확인해보십시오.

table widget\_example | eval url=if(isnotnull(query), concat("https://example.com", path, "?", query), concat("https://example.com", path)) | search src\_ip==ip("66.249.79.179")

쿼리 실행

쿼리 실행은 클릭 또는 드래그 이벤트가 발생했을 때 미리 정의해놓은 이벤트 쿼리를 "**[쿼리 > 쿼리](query)**"에서 실행하는 기능입니다. 이벤트 쿼리는 클릭 또는 드래그 이벤트 시점에 예약어로 지정된 정보를 받아서 쿼리를 실행하도록 구성하는 것이 일반적입니다.



예약어

쿼리 실행에 사용할 수 있는 예약어는 다음 표와 같습니다.

|  |  |  |
| --- | --- | --- |
| 이벤트 | 예약어 | 설명 |
| 클릭 | $필드이름$ | 이름으로 지정된 필드의 값(예: $method$) |
| 클릭 | $series$ | 종속 변수 필드의 이름 |
| 드래그 | $xfield$ | 독립 변수 필드의 이름 |
| 드래그 | $from$ | 독립 변수 구간의 시작값 |
| 드래그 | $to$ | 독립 변수 구간의 마지막값 |

* 데이터 쿼리에서 필드 이름을 특정할 수 있으면 $필드이름$으로 이벤트 쿼리를 작성할 수 있습니다.
* 데이터 쿼리에 [timechart](https://docs.logpresso.com/ko/query/timechart-command) 명령처럼 집계 결과를 계산하는 쿼리를 사용하면 필드값을 특정할 수 없으므로 $series$로 필드 이름을 가져오도록 이벤트 쿼리를 작성하십시오.

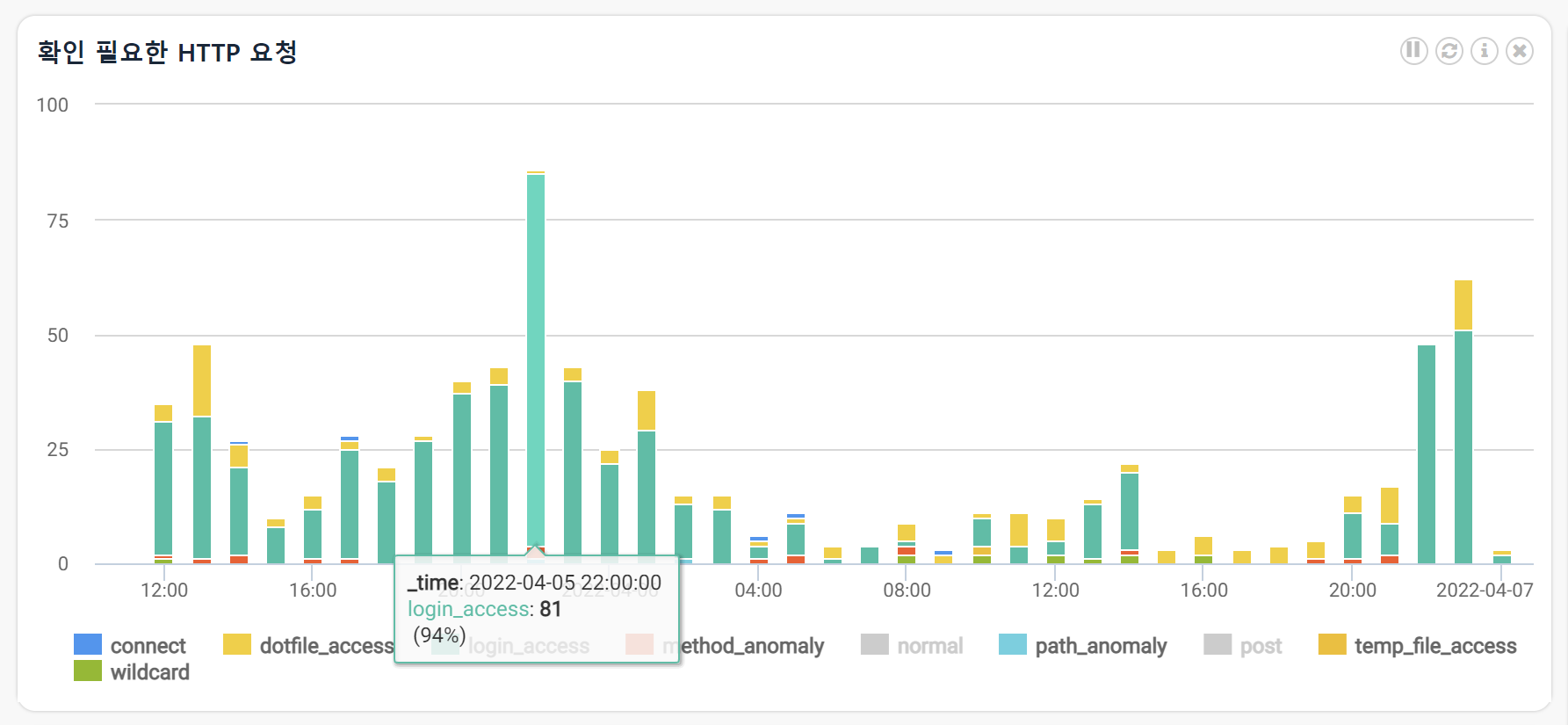
예제

이 예제의 목표는 사용자가 위젯에서 **suspicious** 필드를 누르면, 사용자가 눌러서 선택한 유형의 HTTP 요청이 시간당 얼마나 발생했는지, 시간 대역을 드래그해서 선택하면 해당 시간대 동안 확인이 필요한 HTTP 요청이 유형별로 얼마나 발생했는지 보여주는 것입니다.

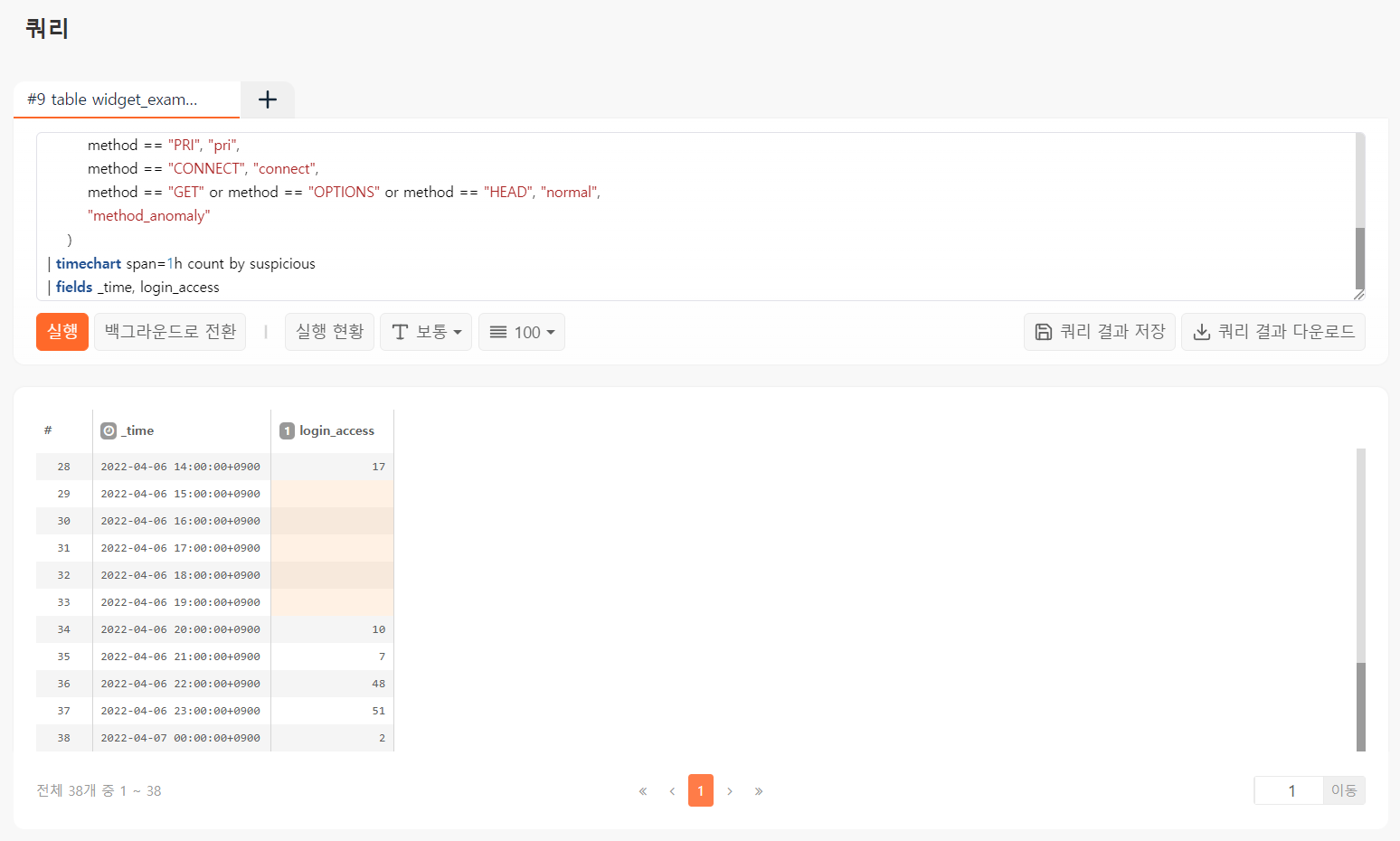
[누적 세로 막대 차트 예제](https://docs.logpresso.com/ko/enterprise/4.0/ui/chart-bar-vertical-acc)를 참고하여 위젯을 추가합니다. 위젯을 설정할 때 다음과 같이 이벤트 속성을 지정합니다.

* **클릭**: 쿼리 실행
* table widget\_example | eval suspicious = case( path == "\*/../\*" or path == "\*/./\*", "dir\_traversal", path == "/.\*", "dotfile\_access", path == "/temp\*" or path == "/tmp\*", "temp\_file\_access", path == "/bbs/login\*", "login\_access", path == "\\\*", "path\_anomaly", path == "\\*", "wildcard", method == "POST", "post", method == "PRI", "pri", method == "CONNECT", "connect", method == "GET" or method == "OPTIONS" or method == "HEAD", "normal", "method\_anomaly" ) | timechart span=1h count by suspicious | fields \_time, $series$
* **드래그**: 쿼리 실행
* table widget\_example | eval suspicious = case( path == "\*/../\*" or path == "\*/./\*", "dir\_traversal", path == "/.\*", "dotfile\_access", path == "/temp\*" or path == "/tmp\*", "temp\_file\_access", path == "/bbs/login\*", "login\_access", path == "\\\*", "path\_anomaly", path == "\\*", "wildcard", method == "POST", "post", method == "PRI", "pri", method == "CONNECT", "connect", method == "GET" or method == "OPTIONS" or method == "HEAD", "normal", "method\_anomaly" ) | timechart span=1h count by suspicious | search $xfield$ >= $from$ and $xfield$ < $to$ and $serires$

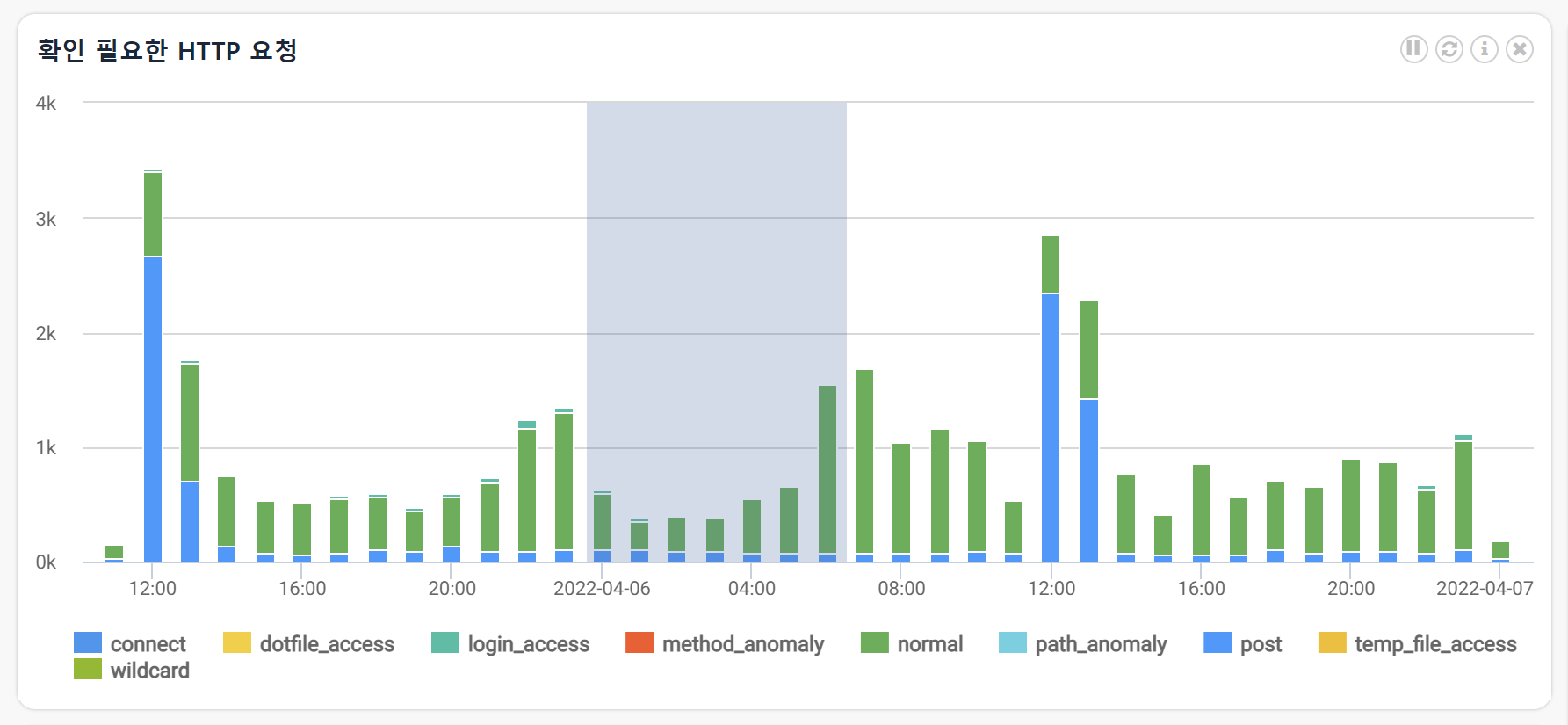
수정한 위젯에서 임의로 세로 막대를 누릅니다.



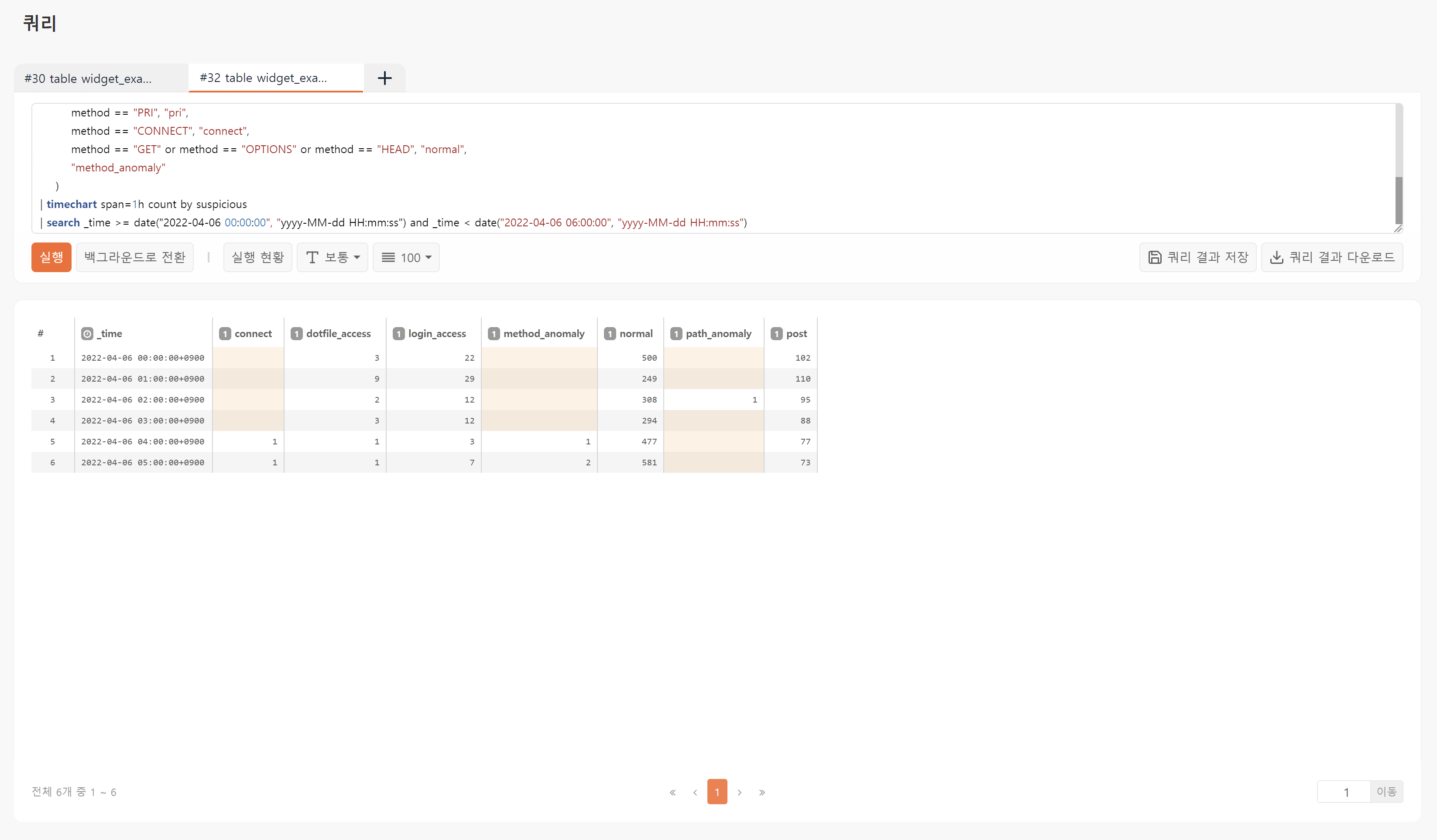
**쿼리 > 쿼리**로 화면이 전환되면서 이벤트 쿼리문이 실행됩니다. $series$가 클릭 이벤트가 발생한 데이터 항목의 필드 이름인 login\_access로 치환되어 실행된 것을 확인할 수 있습니다.



수정한 위젯에서 특정한 구간을 드래그하여 선택합니다.



**쿼리 > 쿼리**로 화면이 전환되면서 이벤트 쿼리문이 실행됩니다. $xfields$가 $\_time$으로, $from$가 date("2022-04-06 00:00:00", "yyyy-MM-dd HH:mm:ss"), $to$가 date("2022-04-06 06:00:00", "yyyy-MM-dd HH:mm:ss")로 치환되어 실행된 것을 확인할 수 있습니다.



필터링

필터링은 위젯에서 클릭하거나 드래그해서 선택한 "독립 변수의 값"을 기준으로 데이터의 범위를 좁혀서 보는 것을 의미합니다. 필터링이 적용되는 위치는 위젯이 사용하는 '[데이터소스](https://docs.logpresso.com/ko/enterprise/4.0/ui/dashboard-tutorial)'입니다. 데이터소스로 정의된 쿼리를 실행한 후 필터링 쿼리를 적용해 데이터의 범위를 좁혀나갑니다.

필터링은 데이터소스를 사용하는 모든 위젯에 적용됩니다. 프리셋 안에서 다른 탭 패널에 있는 위젯들도 필터링의 영향을 받습니다.



드래그 이벤트에 필터링을 설정하려면 독립 변수의 필드 유형이 '시간'이어야 합니다.

예약어

필터링에 사용할 수 있는 예약어는 다음 표와 같습니다.

|  |  |  |  |
| --- | --- | --- | --- |
| 이벤트 | 예약어 | 설명 | 사용 위치 |
| 클릭 | $x$ | 독립 변수 필드의 값 | 이벤트 쿼리 |
| 드래그 | $xfield$ | 독립 변수 필드의 이름 | 이벤트 쿼리 |
| 드래그 | $from$ | 독립 변수 구간의 시작값 | 이벤트 쿼리 |
| 드래그 | $to$ | 독립 변수 구간의 마지막값 | 이벤트 쿼리 |
| 클릭, 드래그 | $drilldown$ | 이벤트 쿼리를 삽입할 위치 | 데이터 쿼리 |
| 클릭, 드래그 | $filter$ | 이벤트 쿼리를 삽입할 위치 | 데이터 쿼리(그리드 위젯) |

필터링에 사용되는 이벤트 쿼리는 대부분 [search](https://docs.logpresso.com/ko/query/search-command) 명령을 사용합니다. 이벤트 쿼리는 데이터소스로 지정한 쿼리의 결과를 입력으로 받아서 처리합니다. 이것은 데이터소스 쿼리문의 마지막에 "| $drilldown$"이 있는 것과 같습니다.

필터링을 데이터소스가 아니라 데이터 쿼리에 적용하려면 데이터 쿼리의 특정한 위치에 "| $drilldown$ |"과 같이 예약어를 이용한 쿼리 구문을 삽입하십시오. 이렇게 하면 데이터소스가 아니라 데이터 쿼리에 필터링이 적용됩니다.

$filter$는 그리드 위젯에서 사용하는 예약어로, 데이터소스의 사용 여부와 무관하게 데이터 쿼리에 삽입할 수 있습니다.

예약어를 사용하지 않고 필터링 동작을 **기본값**으로 설정해두면 클릭한 위치에서, 드래그한 구간의 시작/끝에서 독립 변수의 값을 읽어와 필터링을 적용합니다.

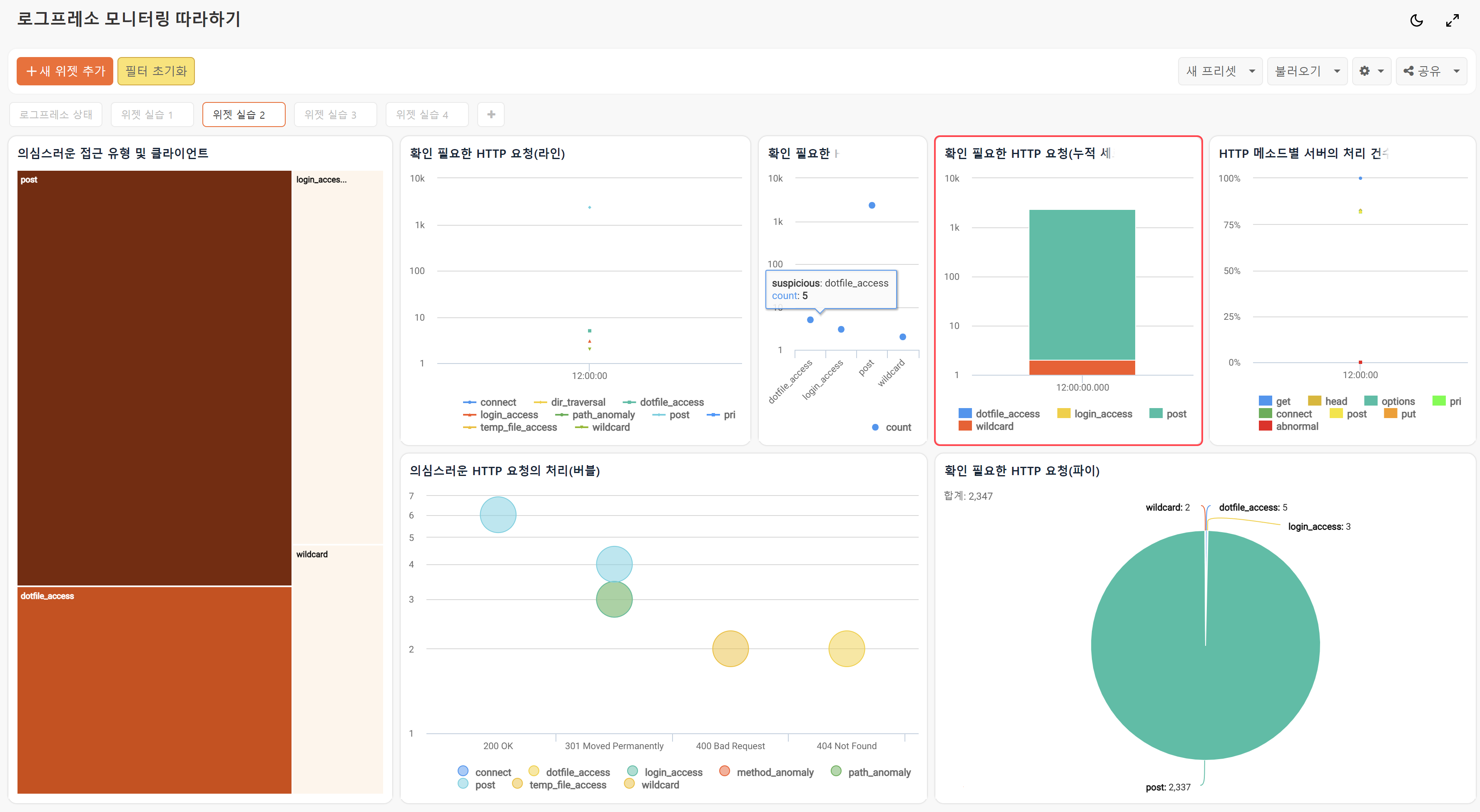
예제

이 예제의 목적은 데이터소스 쿼리로 데이터를 가져오는 누적 세로 막대 차트에서 클릭 또는 드래그하여 기간을 선택하면 동일한 데이터소스를 사용하는 다른 모든 위젯들이 해당 기간 범위 내에서 정보를 보여주도록 하는 것입니다.

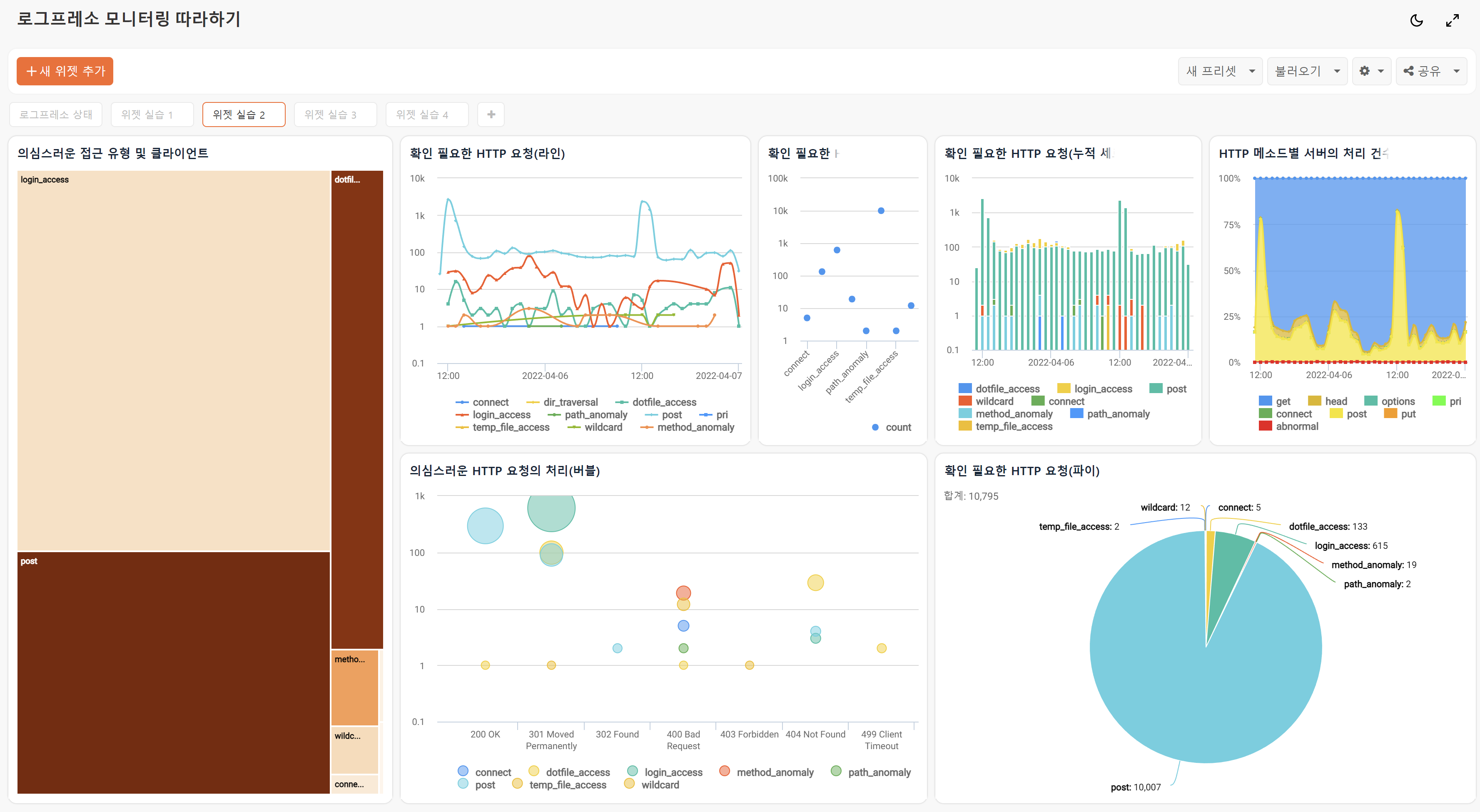
[누적 세로 막대 차트 예제](https://docs.logpresso.com/ko/enterprise/4.0/ui/chart-bar-vertical-acc)에 따라 위젯을 추가한 다음, 다음과 같이 이벤트 속성을 지정합니다.

* **클릭**: 필터링, 사용자 정의 쿼리
* search \_time >= $x$ and \_time < dateadd($x$, "hour", 1)
* **드래그**: 필터링, 사용자 정의 쿼리
* search $xfield$ >=$from$ and $xfield$ < $to$

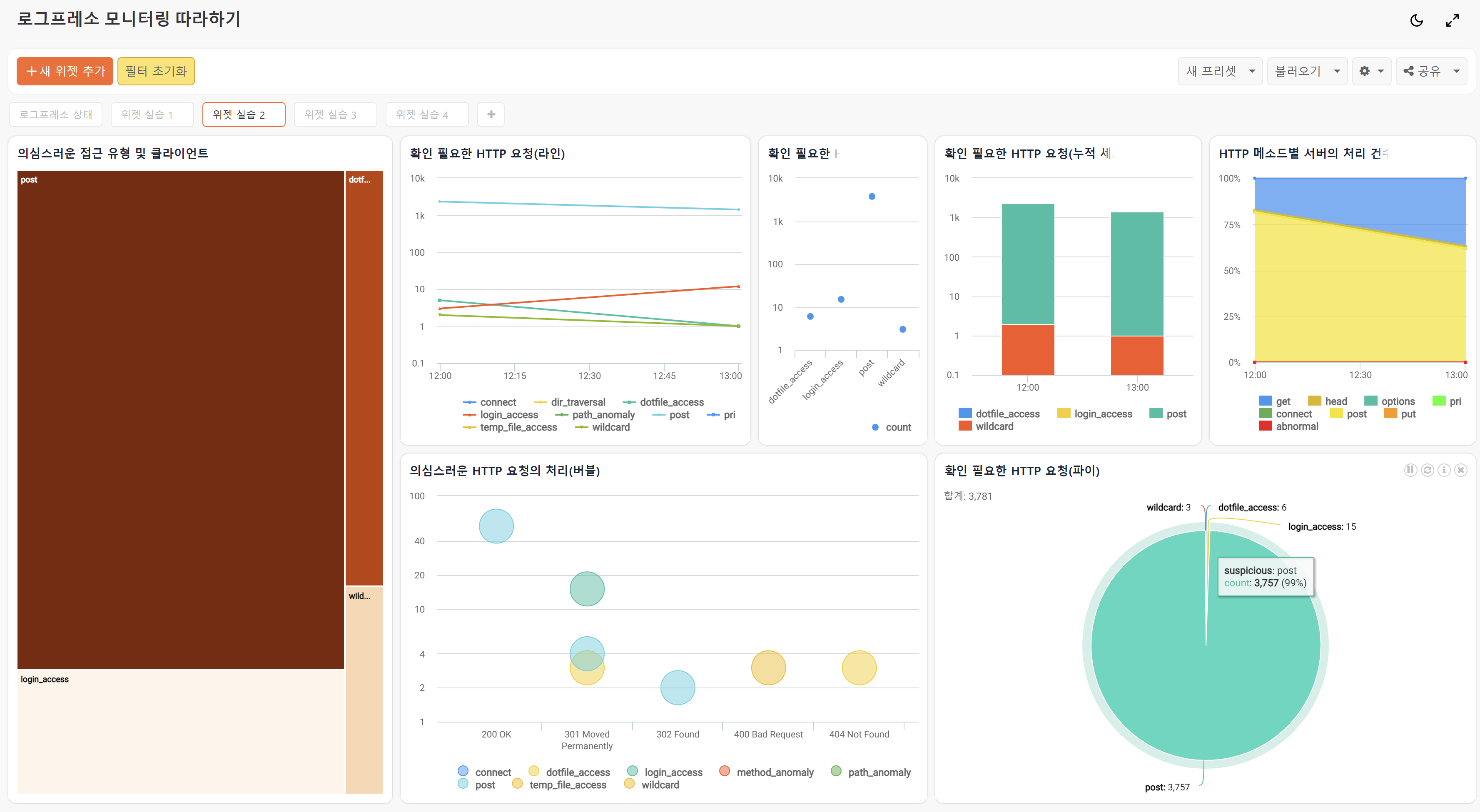
수정한 누적 세로 막대 위젯에서 임의의 세로 막대를 클릭하고, 이벤트 쿼리 결과를 반영해 위젯이 갱신되는 것을 확인합니다. 위젯은 클릭한 항목에 해당하는 1 시간 동안 발생한 데이터만 보여줍니다. 동일한 데이터소스를 사용하는 다른 위젯들도 새로고침 주기에 따라 데이터를 갱신할 때 동일한 필터링이 적용되는 것을 확인할 수 있습니다.



[대시보드 도구모음](https://docs.logpresso.com/ko/enterprise/4.0/ui/dashboard-intro)에서 **필터 초기화**를 누르고 대시보드에 적용된 필터가 해제된 것을 확인합니다.



수정한 위젯에서 특정한 구간을 드래그하여 선택하고, 이벤트 쿼리 결과를 반영해 위젯이 갱신되는 것을 확인합니다. 위젯은 드래그해서 선택한 구간에 해당하는 시간 동안 발생한 데이터만 보여줍니다. 동일한 데이터소스를 사용하는 다른 위젯들도 새로고침 주기에 따라 데이터를 갱신할 때 동일한 필터링이 적용되는 것을 확인할 수 있습니다.



백그라운드 쿼리 실행

백그라운드 쿼리 실행은 그리드 위젯에서 사용할 수 있는 이벤트 동작으로, 백그라운드에서 쿼리를 실행하고, 해당 쿼리 결과를 반영해서 한꺼번에 모든 위젯을 갱신하여 보여줍니다.

이 이벤트 동작은 로그프레소 플랫폼의 이벤트 연관 분석(CEP, Complex Event Processing) 기능을 이용해서 사용하는 경우가 많습니다. 그리드 위젯에서 백그라운드 쿼리를 이용해 CEP의 특정 토픽에 키-값을 등록하고, 다른 위젯에서 이 값을 참조하도록 쿼리를 구성하면 그리드에서 발생하는 이벤트를 기준으로 대시보드의 위젯 정보를 동시에 업데이트할 수 있습니다. 백그라운드 쿼리는 쿼리가 완료되는 시점에 대시보드 탭 화면에 있는 모든 위젯의 업데이트를 할 수 있다는 점에서 쿼리 실행과 차이가 있습니다.

이 기능을 제대로 활용하려면 [이벤트 연관 분석](https://docs.logpresso.com/ko/query/section-event-correlation) 명령어들과 [이벤트 컨텍스트 함수](https://docs.logpresso.com/ko/query/section-complex-event-processing-functions)에 대한 이해가 필요합니다.

예약어

위젯은 각각 고유한 이벤트 예약어를 사용할 수 있습니다.

|  |  |  |  |
| --- | --- | --- | --- |
| 예약어 | 설명 | 트리거 | 사용 위치 |
| $필드이름$ | 이름으로 지정된 필드의 값 | 클릭 | 이벤트 쿼리 |
| $series$ | 종속 변수 필드의 이름 | 클릭 | 이벤트 쿼리 |

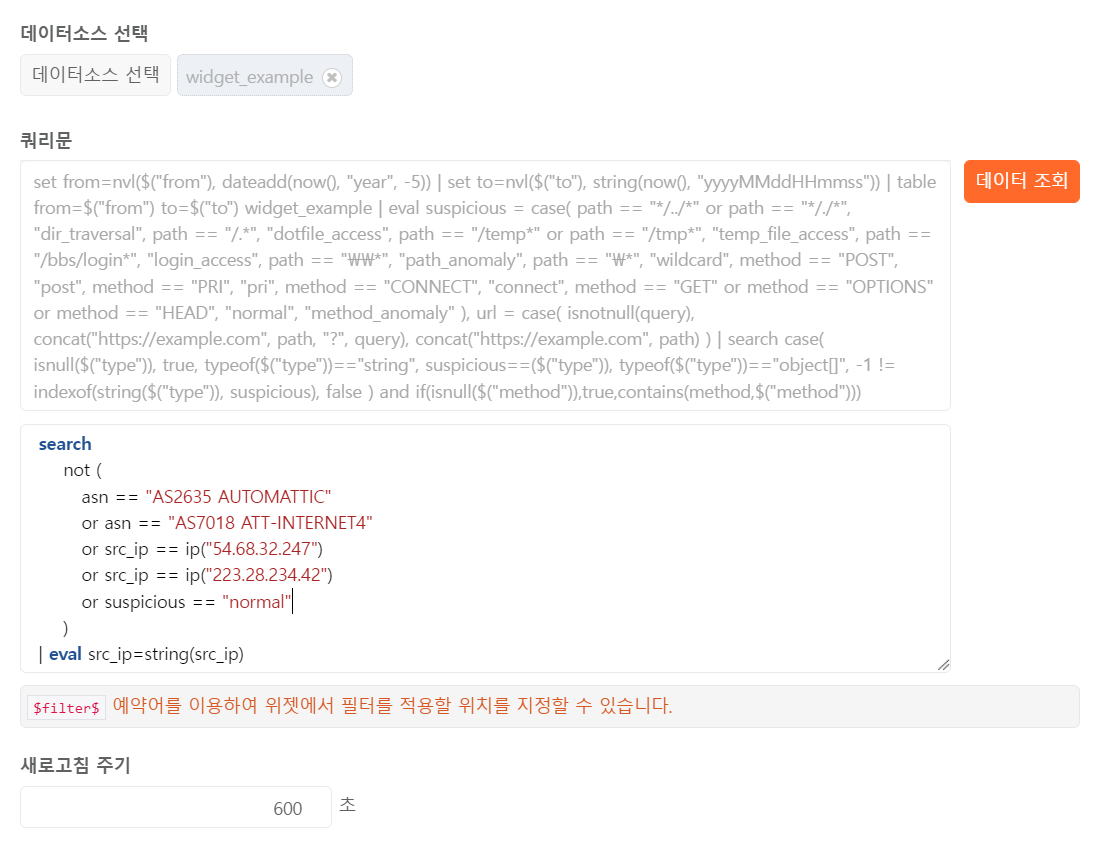
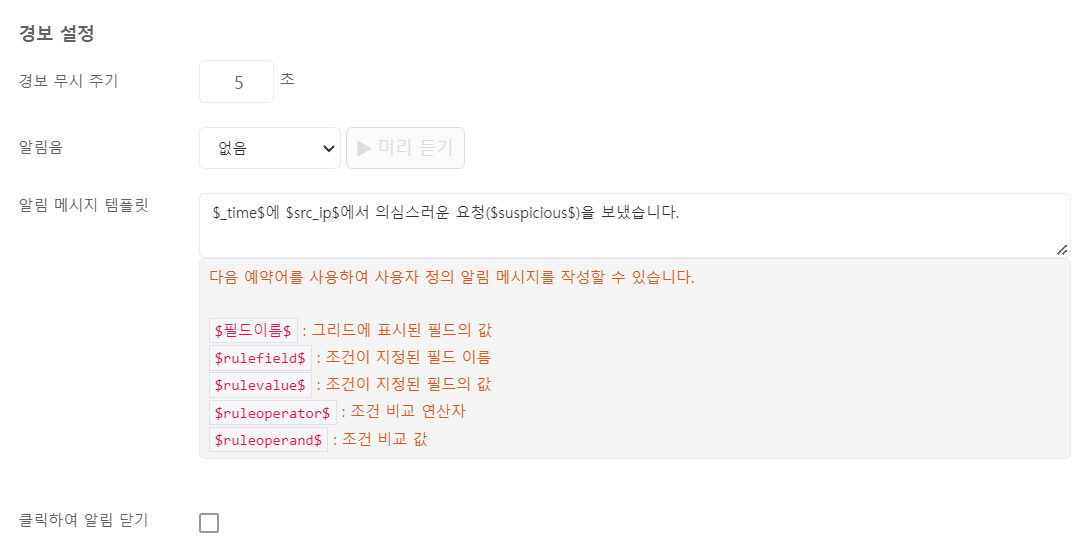
예제

이 예제의 목적은 CEP 기능을 활용해 탭 패널의 모든 위젯이 동시에 동작하도록 하는 것입니다.

먼저 탭 패널을 추가하고, 새 탭 패널에서 예제를 따라해보시기 바랍니다.

이름이 "백그라운드 쿼리 실습"인 [탭 패널을 추가](https://docs.logpresso.com/ko/enterprise/4.0/ui/dashboard-usage)합니다.

패널에 다음과 같은 속성을 갖는 [그리드 위젯](https://docs.logpresso.com/ko/enterprise/4.0/ui/data-widget-grid)을 추가합니다.

* **위젯 이름**: 의심스러운 웹 클라이언트
* **타입 선택**: 그리드
* **데이터소스 선택**: [widget\_example](https://docs.logpresso.com/ko/enterprise/4.0/ui/dashboard-data-for-widget-drill)
* **쿼리문**
* search not ( asn == "AS2635 AUTOMATTIC" or asn == "AS7018 ATT-INTERNET4" or src\_ip == ip("54.68.32.247") or src\_ip == ip("223.28.234.42") or suspicious == "normal" ) | eval src\_ip=string(src\_ip)
* **새로고침 주기**: 600초
* 
* **필드 순서**
* 다음 필드만 선택하여 순서대로 정렬: \_time, src\_ip, asn, country, suspicious, method, path, query, status
* **src\_ip**에 이벤트 설정
* **이벤트 동작**: 백그라운드 쿼리 실행
* **쿼리문**
* table widget\_example | search src\_ip == ip($src\_ip$) | eval category = case( path == "\*/../\*" or path == "\*/./\*", "dir\_traversal", path == "/.\*", "dotfile\_access", path == "/temp\*" or path == "/tmp\*", "temp\_file\_access", path == "/bbs/login\*", "login\_access", path == "\\\*", "path\_anomaly", path == "\\*", "wildcard", method == "POST", "post", method == "PRI", "pri", method == "CONNECT", "connect", method == "GET" or method == "OPTIONS" or method == "HEAD", "normal", "method\_anomaly" ), src\_ip=str(src\_ip) | search category != "normal" | evtctxadd topic=$src\_ip$ key=category timeout=600s src\_ip == $src\_ip$
* **새로고침**: '쿼리 실행 완료 후 모든 위젯 새로고침' 선택
* 
* **경보 무시 주기**: 5초
* **알림음**: 없음
* **알림 메시지 템플릿**: $\_time$에 $src\_ip$에서 의심스러운 요청($suspicious$)을 보냈습니다.
* **클릭하여 알림 닫기**: 선택 해제
* 

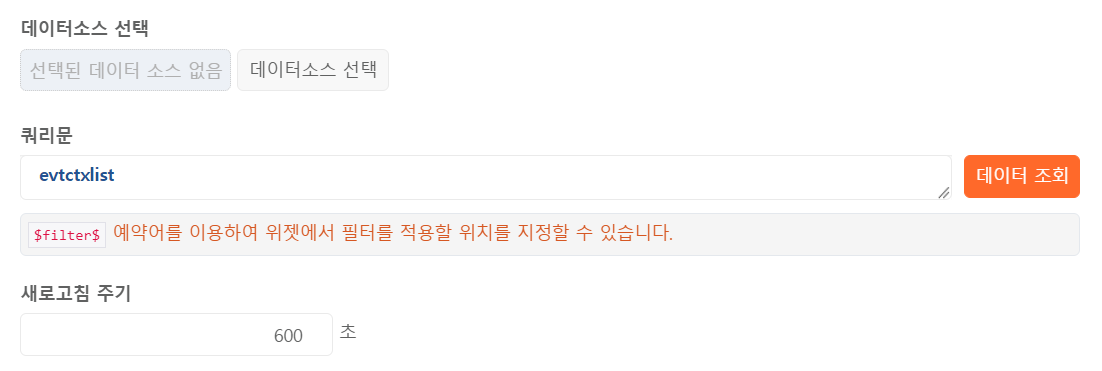
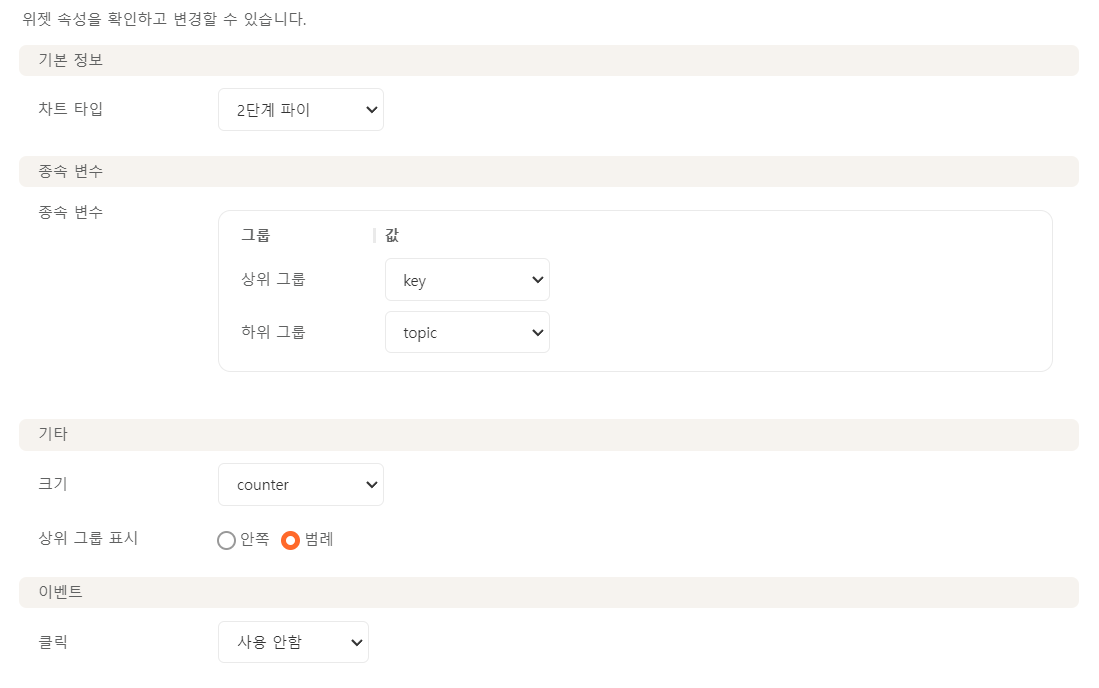
그리드 위젯에서 백그라운드 쿼리가 실행되었을 때 함께 사용할 경고 상자 위젯을 추가합니다.

* **위젯 이름**: 의심 사례
* **타입 선택**: 경고 상자
* **데이터소스 선택**: 선택 안 함
* **쿼리문**
* evtctxlist | stats sum(counter) as occurrence
* **새로고침 주기**: 600초
* 
* **타입**: 필드값
* **목표 필드**: occurrence
* **표시 필드**: occurrence
* **배경색 조건**

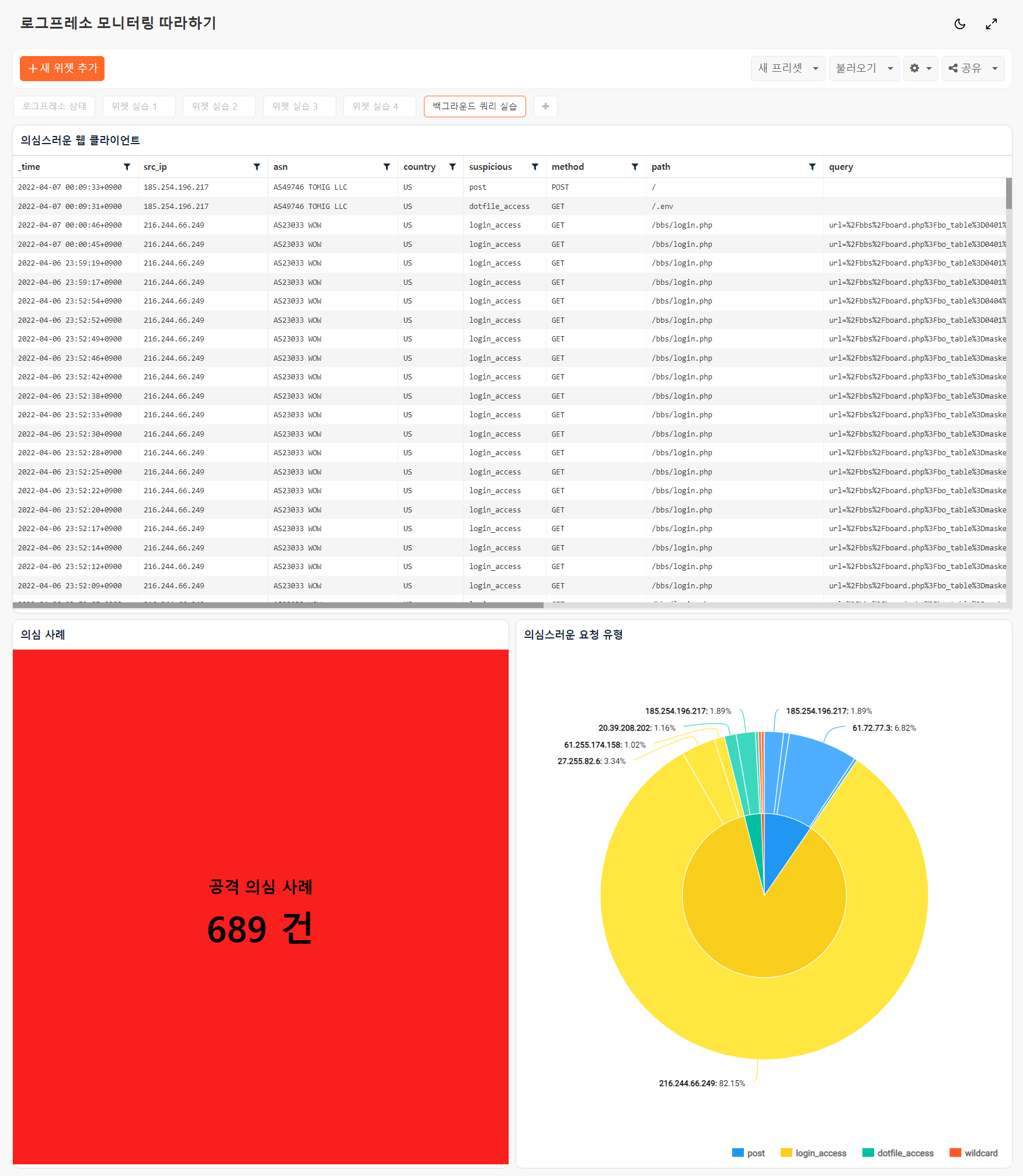
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 조건식 | 임계치 | 글자 | 배경 | 동작 |
| = | 0 | 임의의 색 선택 | 임의의 색 선택 | 경고음: 없음, 알림 메시지: 선택 |
| > | 0 | 임의의 색 선택 | 임의의 색 선택 | 경고음: 없음, 알림 메시지: 선택 |

* **클릭하여 알림 닫기**: 선택 해제
* **기본 배경색**: 기본색 사용
* **기본 텍스트**: 사용 안 함
* **라벨 글자 크기**: 기본값
* **텍스트 글자 크기**: 36pt
* **라벨**: 의심 사례
* **접두사**: 없음
* **접미사**: 건
* **천 단위 쉼표**: 선택
* **소수점 표시**: 선택 해제
* 

그리드 위젯에서 백그라운드 쿼리가 실행되었을 때 함께 사용할 2단계 파이 차트 위젯을 추가합니다.

* **위젯 이름**: 의심스러운 요청 유형
* **타입 선택**: 차트
* **데이터소스 선택**: 선택 안 함
* **쿼리문**
* evtctxlist
* **새로고침 주기**: 600초
* 
* **차트 타입**: 2단계 파이
* **종속 변수**
* **상위 그룹**: key
* **하위 그룹**: topic
* **크기**: counter
* **상위 그룹 표시**: 범례
* **클릭**: 사용 안함
* 

모든 위젯을 추가하고 다음 그림과 같이 탭 패널을 구성합니다.



그리드 위젯에서 임의의 **src\_ip** 필드를 누르고, 경고 상자 위젯과 2단계 파이 차트 위젯이 보여주는 정보가 동시에 갱신되어 나타나는 지 확인합니다.