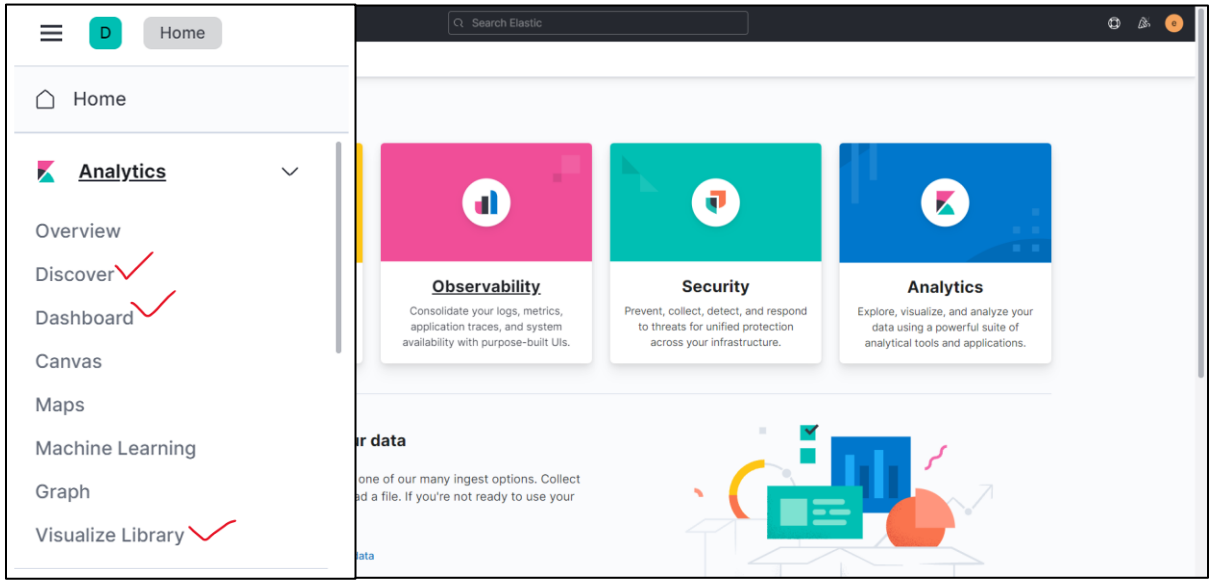
Kibana 시각화

Discover, Dashboard, Visualize Library 살펴보기



Mitre ATT&CK 프레임워크 매핑 필터 사용하기

- 기존에 사용되는 Sysmon 제거하기

  (Sysmon-logstash 연결 때 수행했던 Sysmon 설정 제거)

  - 관리자모드로 cmd를 열고 sysmon.exe -u 수행

```
C:₩Users₩ksj7r₩Desktop₩winlogbeat-7.15.0-windows-x86_64>sysmon.exe -u


System Monitor v13.24 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2021 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Stopping Sysmon.
Sysmon stopped.
Sysmon removed.
Stopping SysmonDrv..
SysmonDrv stopped.
SysmonDrv removed.
Removing service files.......
```

Mitre ATT&CK 프레임워크 매핑 필터 사용하기

- https://github.com/olafhartong/sysmon-modular 다운로드
  - 파워쉘에서 다음 실행
  - $> git clone https://github.com/olafhartong/sysmon-modular.git
  - $> cd sysmon modular
  - $> . .₩Merge-SysmonXml.ps1
  - $> Merge-AllSysmonXml -Path (Get-ChildItem '[0-9]*₩*.xml') -AsString | Out-File sysmonconfig.xml

Mitre ATT&CK 프레임워크 매핑 필터 사용하기

- 해당 깃 폴더에서 cmd를 열고
  - sysmon.exe -accepteula -i sysmonconfig.xml

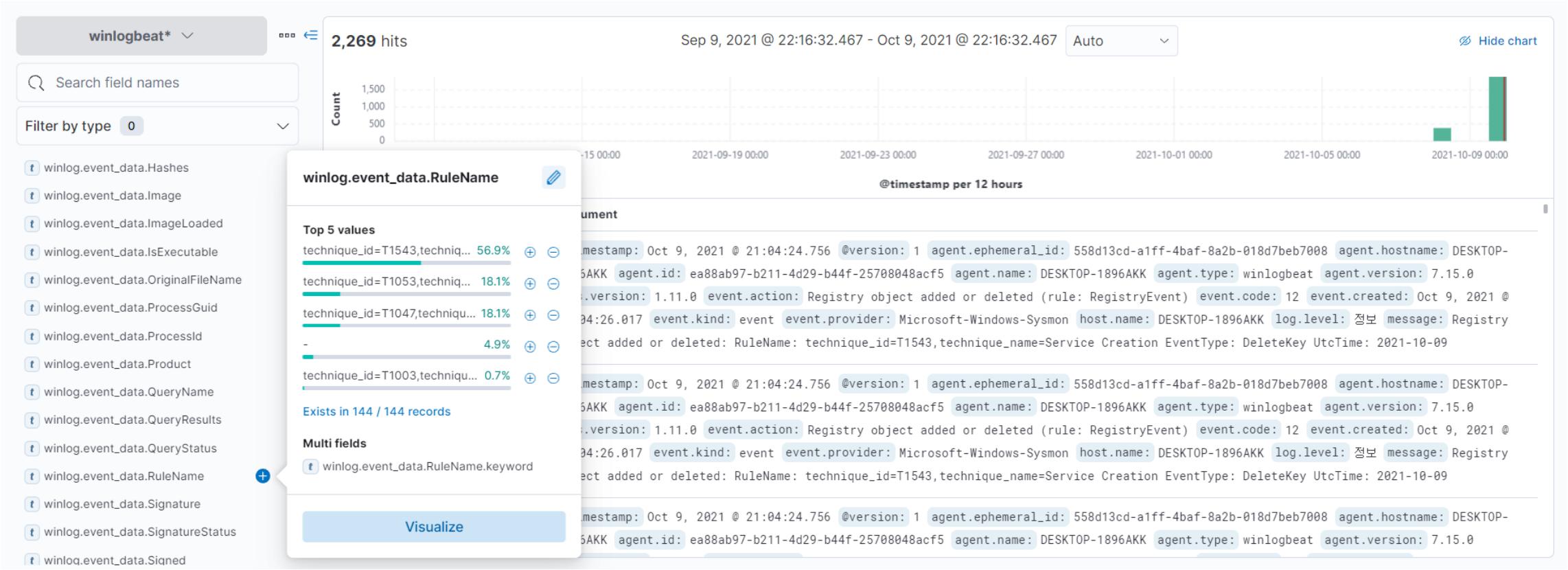
```
C:₩Users₩ksj7r₩sysmon-modular>sysmon.exe -accepteula -i sysmonconfig.xml


System Monitor v13.24 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2021 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.60
Sysmon schema version: 4.70
Configuration file validated.
Sysmon installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon..
Sysmon started.
```

Mitre ATT&CK 프레임워크 매핑 필터 사용하기

- 설정 완료 후 Kibana Discover에서 mitre att&ck와 관련된 정보들이 출력됨을 확인



1. Discover : 데이터 탐색

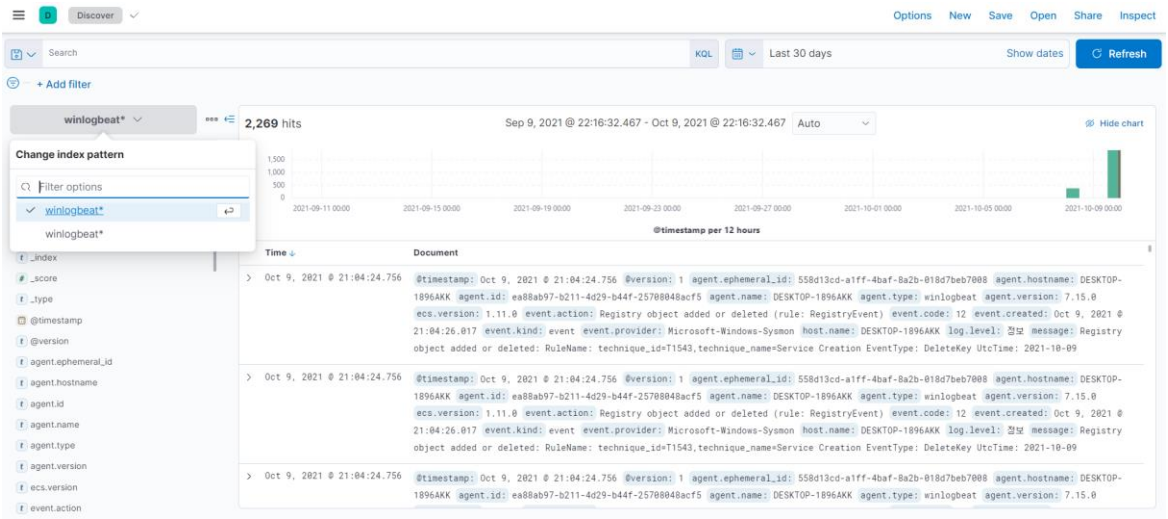
- Discover?
  - Elastic Search의 데이터를 탐색하고 검색 및 질의를 수행할 수 있음
  - 모아진 로그 데이터들을 살펴보고 검색할 수 있는 공간이라고 생각

1. Discover : 데이터 탐색

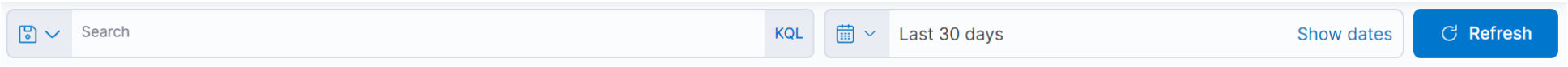
- 데이터 가져오기 - 다음 참고 (Sysmon-logstash 팀 자료조사)
  - https://github.com/K-Shield-Jr/Research/issues/1

  - 위 작업 과정 중 sysmon에 사용되는 xml 파일은 해당 PPT 2~4번 슬라이드를 참고 Mitre ATT&CK 프레임워크 매핑이 설정된 sysmonconfig.xml 사용할 것

1. Discover : 데이터 탐색

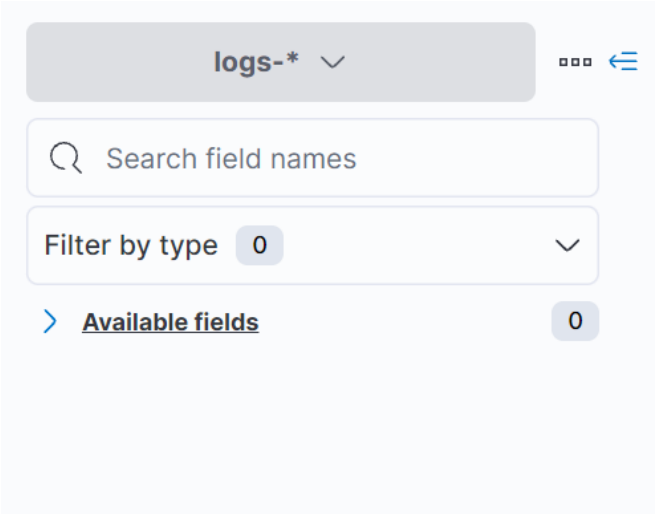


- Discover로 들어가 데이터를 가져오고 생성된 인덱스 패턴을 확인



- 검색할 쿼리, 날짜 조건 입력 하여 데이터 탐색 가능
- Elastic Search 쿼리 문법 가이드
  - https://www.elastic.co/guide/en/elasticsearch/reference/7.15/query-dsl-query-string-query.html#query-string-syntax

1. Discover : 데이터 탐색



- 모든 필드가 표시되지만 Available fields를 설정하면 특정 필드만 표시되게 할 수 있다

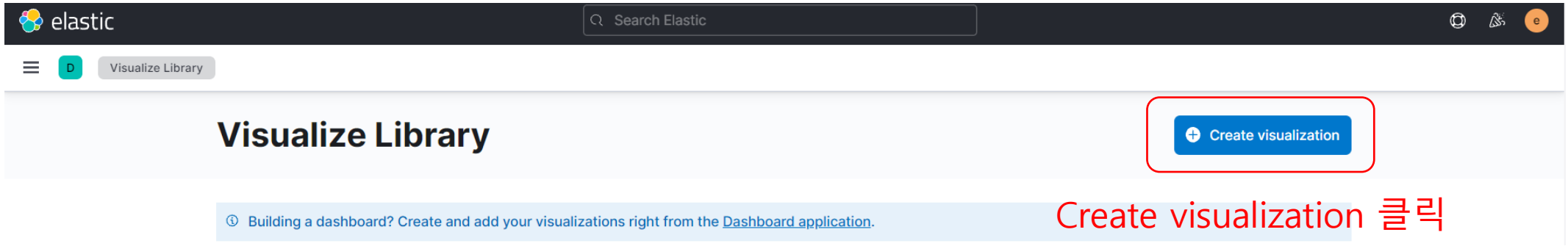
1. Discover : 데이터 탐색

- 키바나 인덱스 패턴?
  - Elastic search는 인덱스 형태로 데이터를 저장/관리

    ➔ DB의 테이블과 비슷한 개념

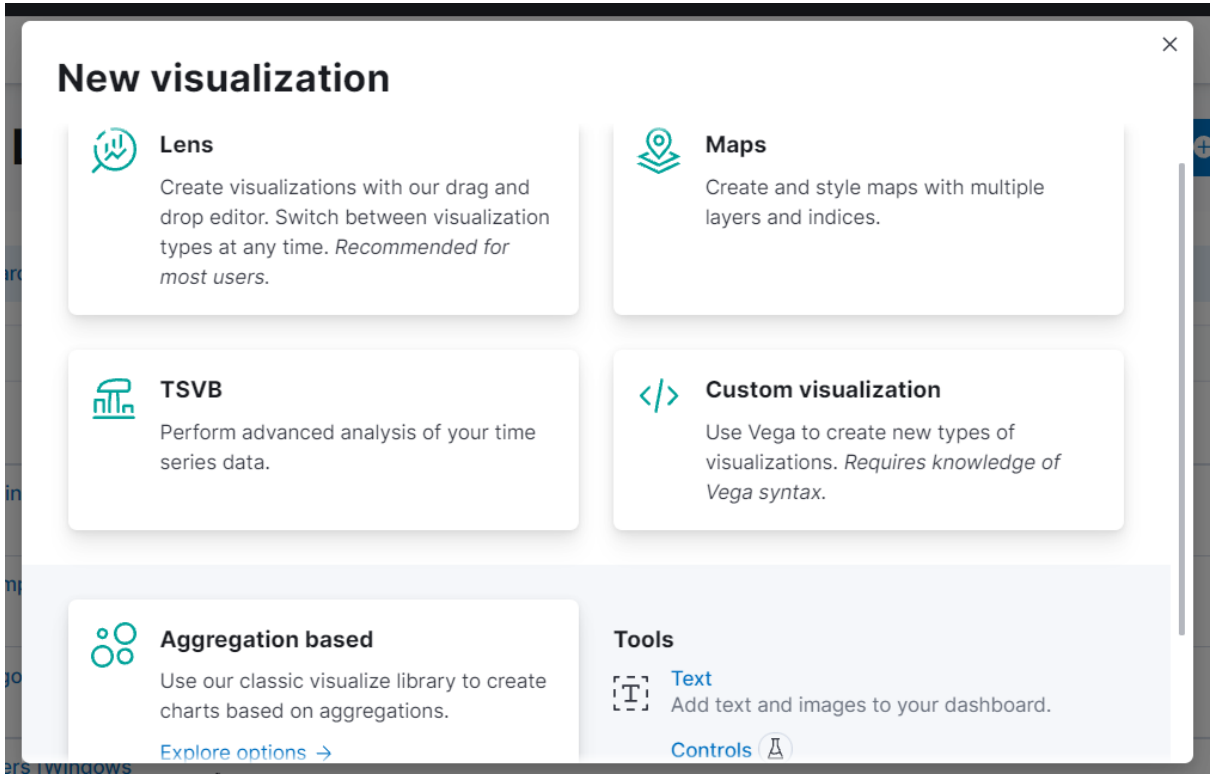
- 인덱스 패턴을 지정하는 이유
  - 사용자가 탐색하고자 하는 데이터를 키바나에 알려주기 위해 지정함

2. Visualize Library : 시각화 자료 만들기



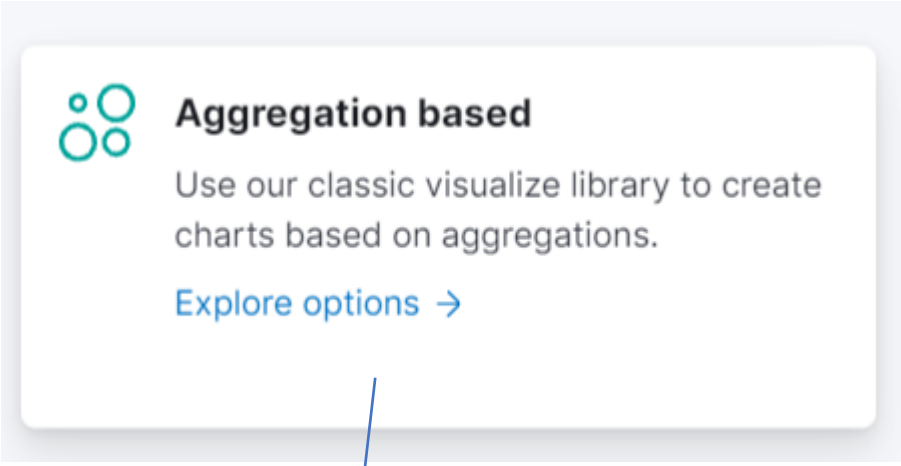
- Visualize를 여러 개 생성해 대시보드의 구성요소로 사용할 수 있음

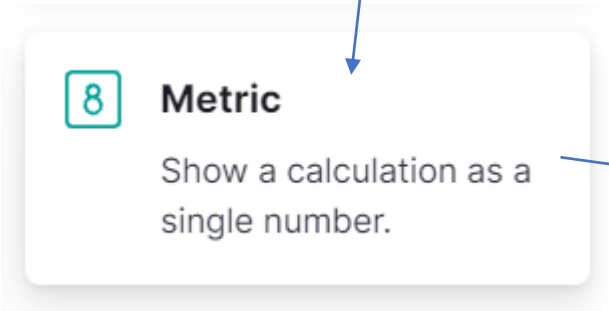
2. Visualize Library : 시각화 자료 만들기



- **Lens** :
  드래그 인 드롭 에디터를 이용해 시각화를 만든다.
  언제든지 Visualizaition들의 타입을 전환할 수 있음
- **Maps** :
  여러 레이어와 인덱스들을 통해 맵 생성 가능
- **TSVB** :
  데이터를 시계열로 시각화 할 수 있음
- **Custom** :
  Vega를 사용해 새 유형의 Visualizations를 만들 수 있음. Vega 문법을 사용할 줄 알아야 함
- **Aggregation based** :
  기존 시각화 라이브러리를 사용해 집계 기반으로 차트 생성 가능

2. Visualize Library : 시각화 자료 만들기



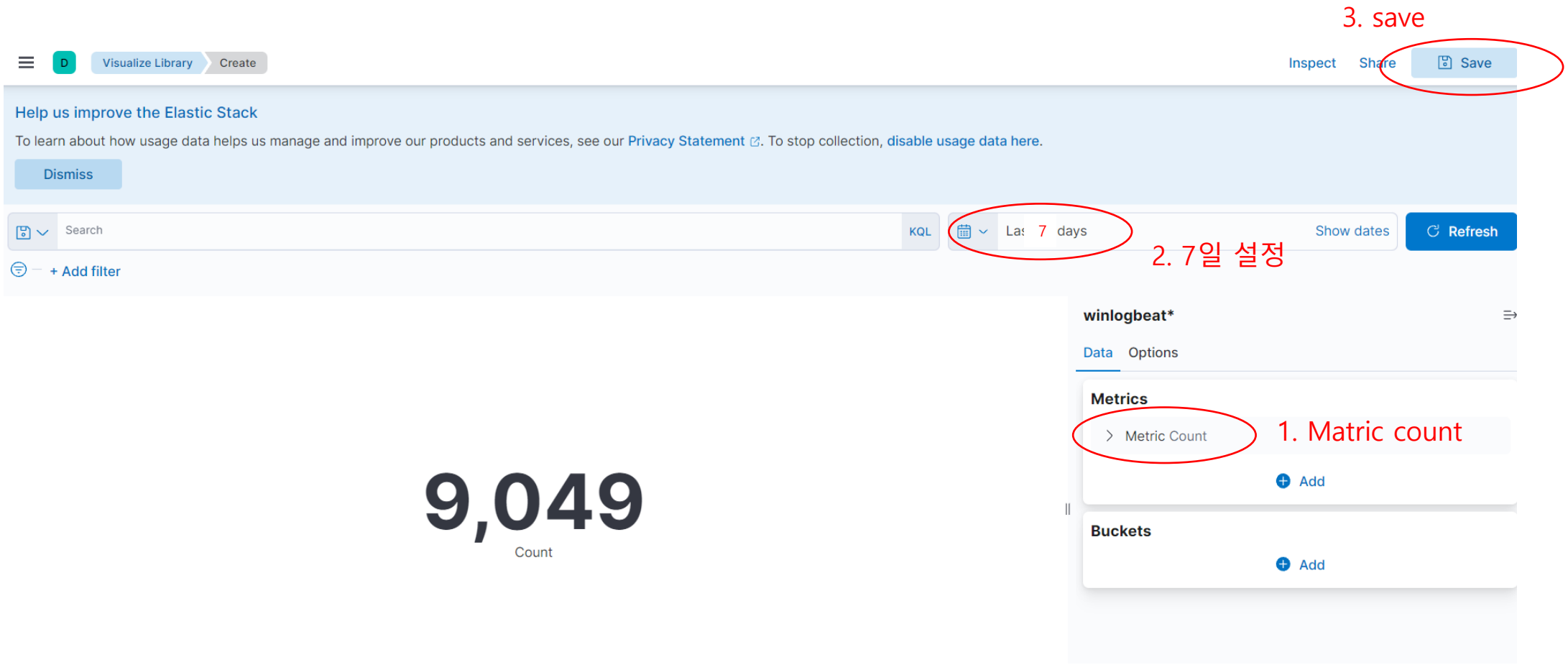


Matric

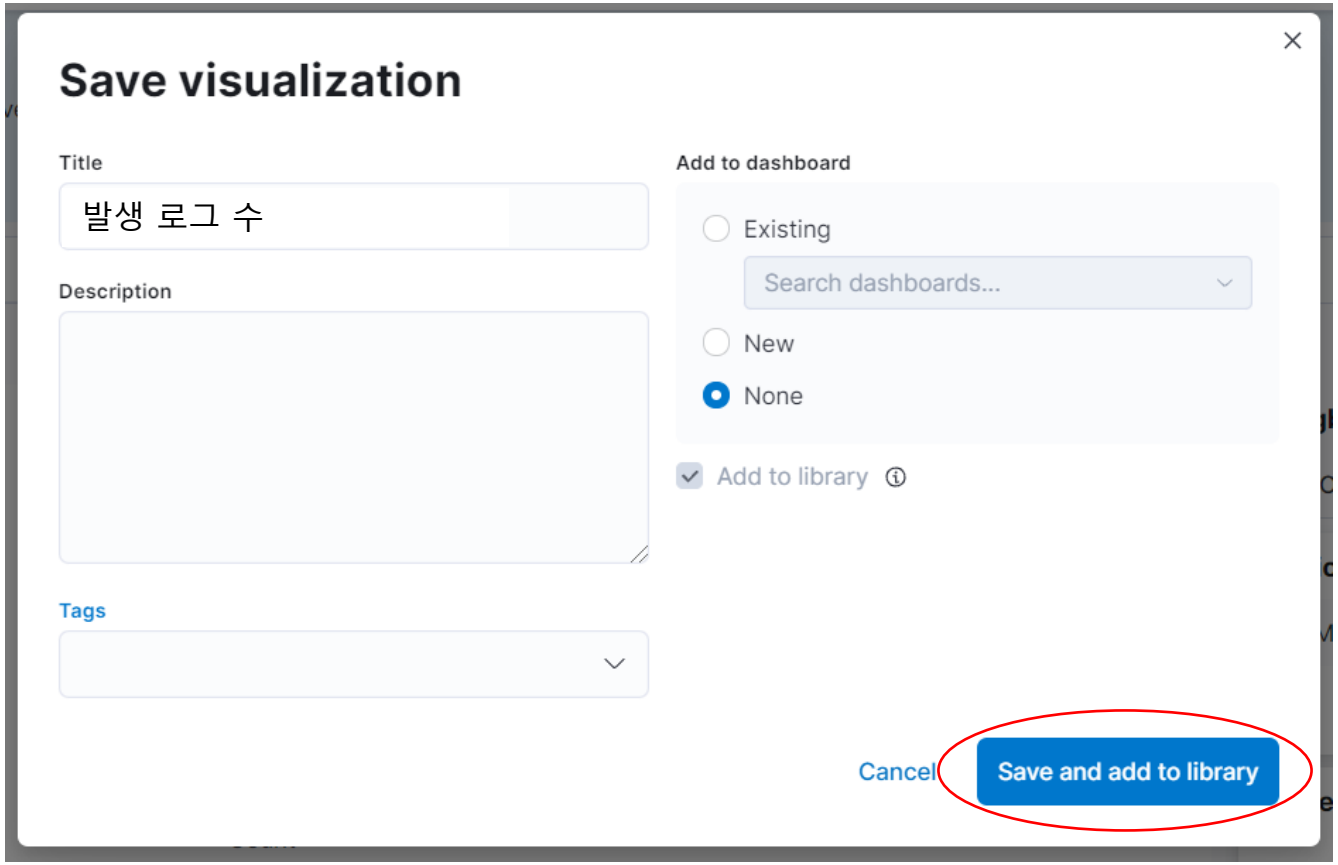
간단한 숫자 세기(count) 설정 가능

ex) 현재 로그가 몇 개 발생했는지,
발생한 event 수

2. Visualize Library : 시각화 자료 만들기

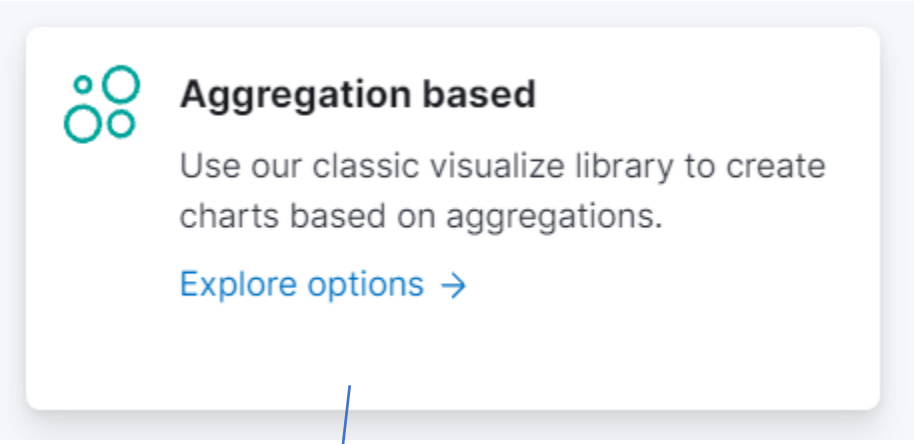


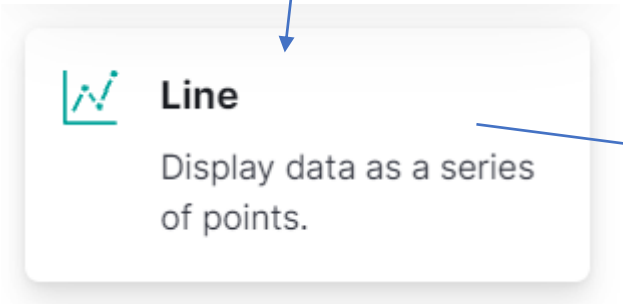
2. Visualize Library : 시각화 자료 만들기

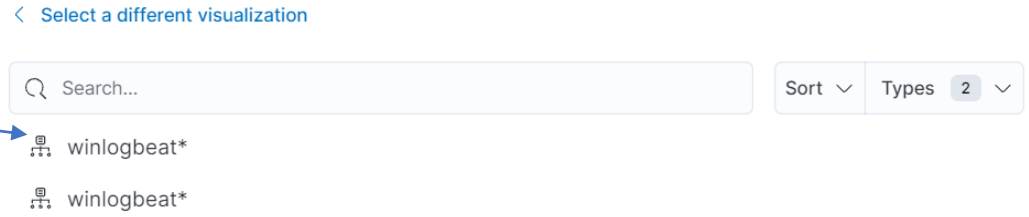


2. Visualize Library : 시각화 자료 만들기

시간대별 로그 그래프 생성

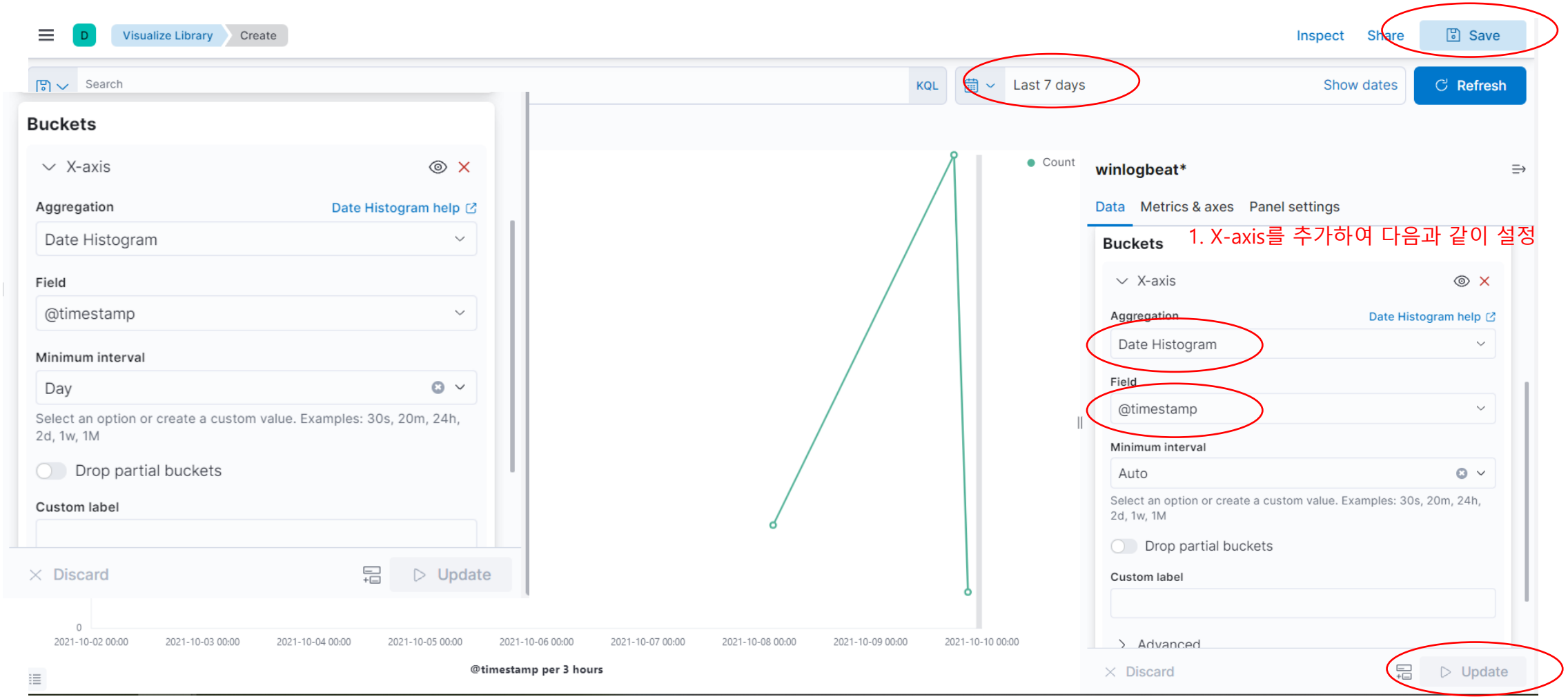






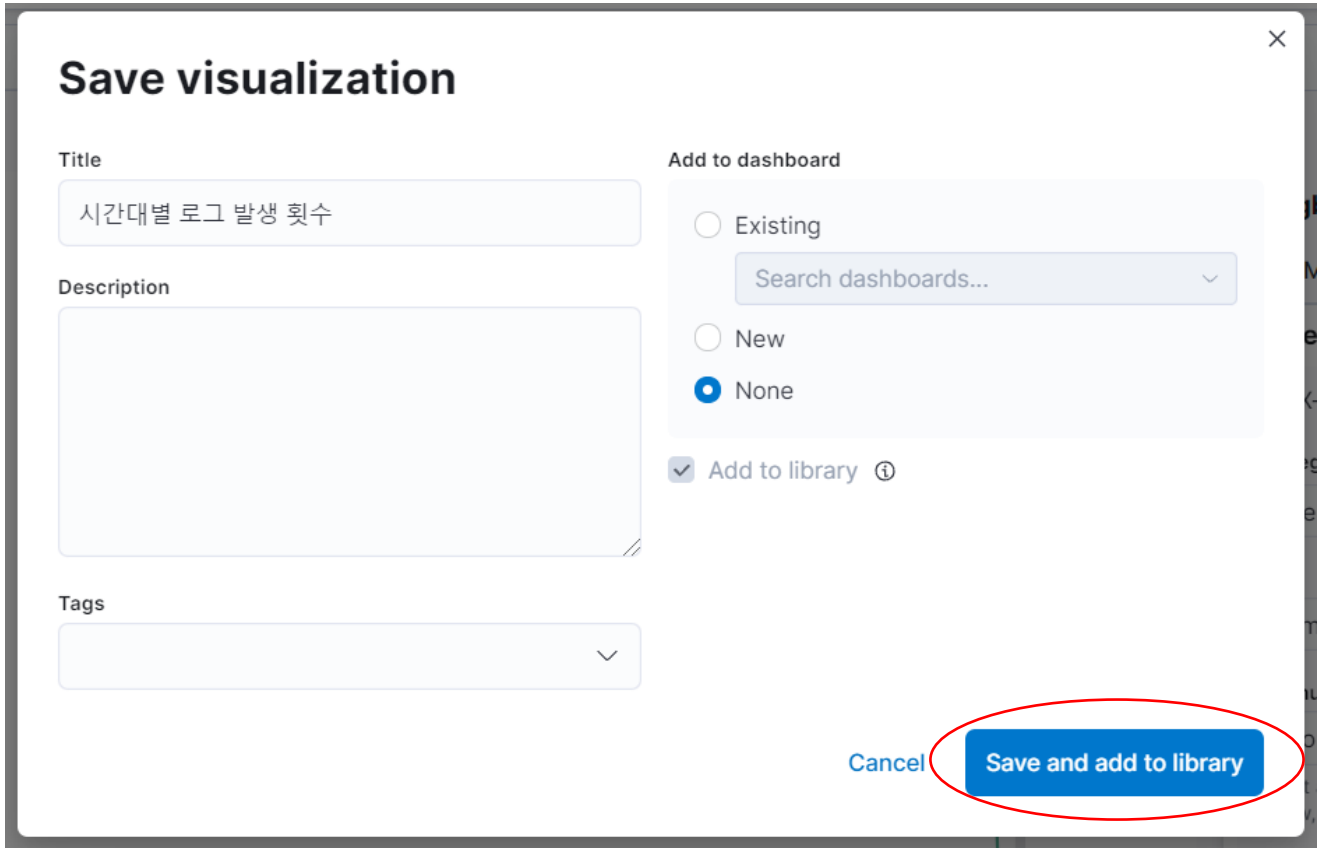
2. Visualize Library : 시각화 자료 만들기

3. save



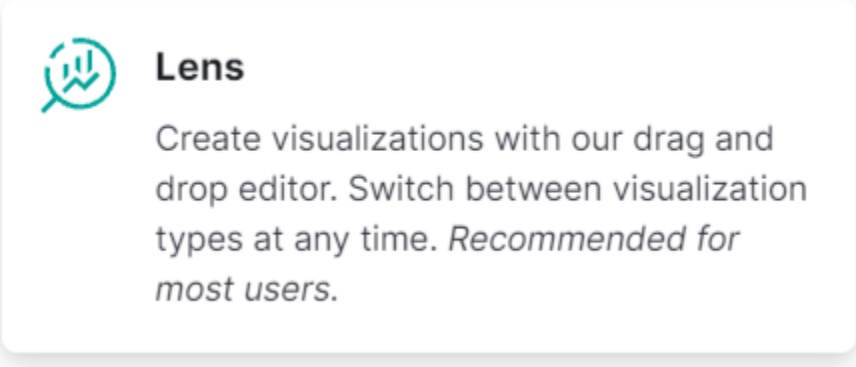
2. Update 클릭

2. Visualize Library : 시각화 자료 만들기

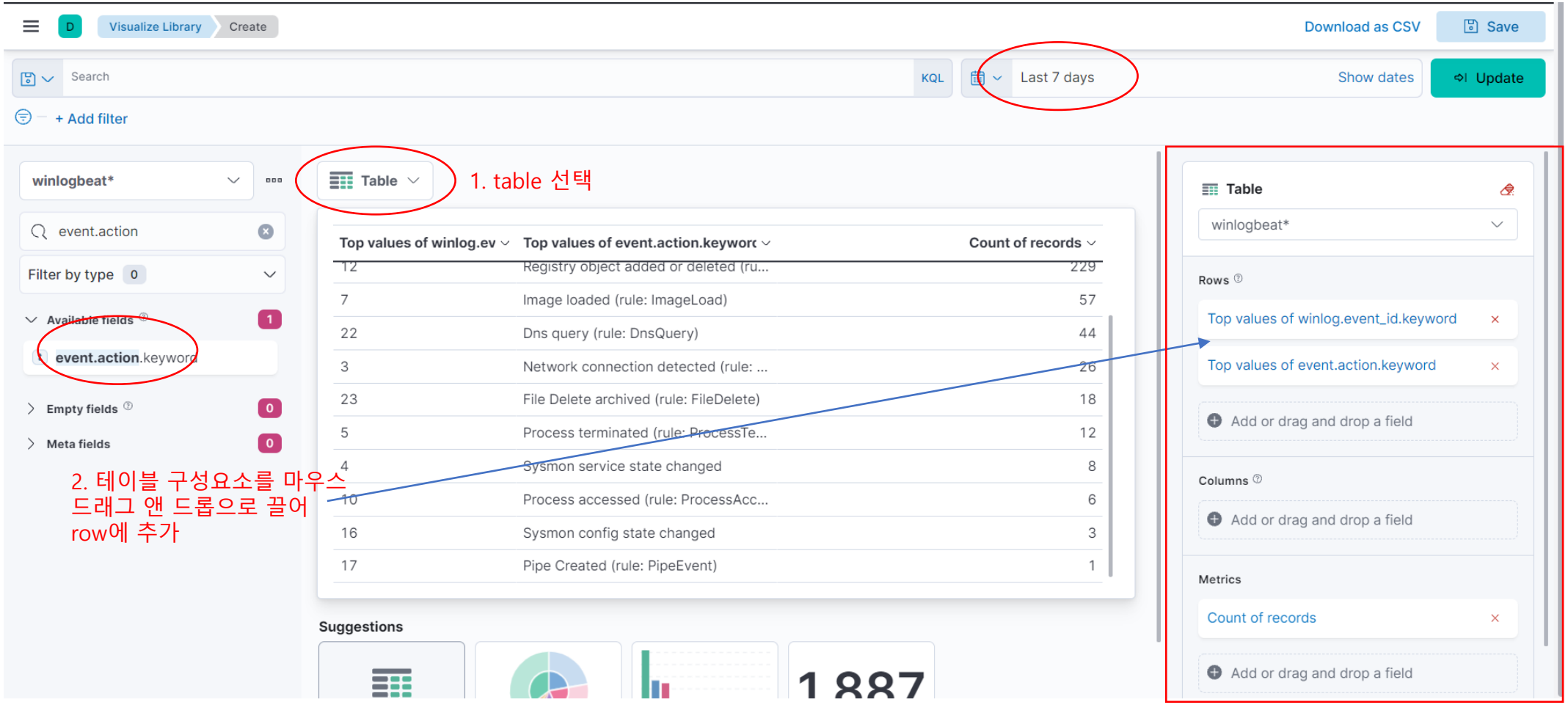


2. Visualize Library : 시각화 자료 만들기

- Lens를 사용해 시각화 하기

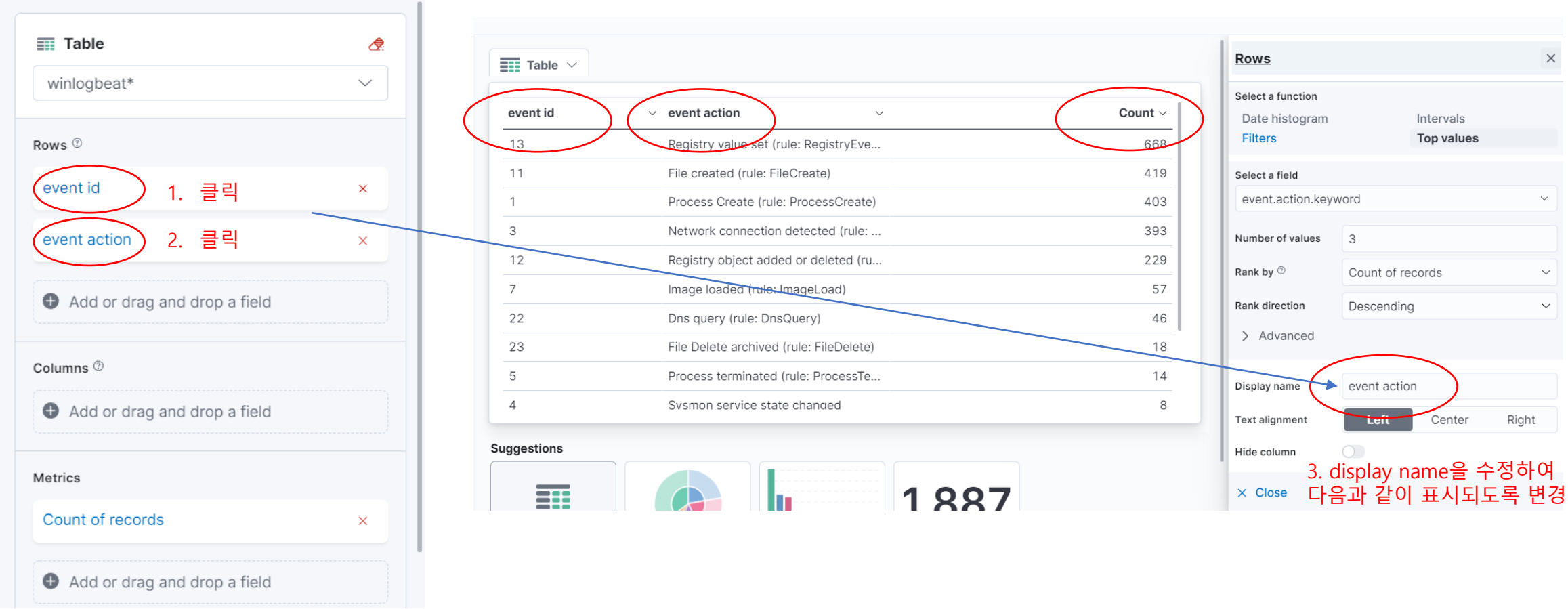


2. Visualize Library : 시각화 자료 만들기

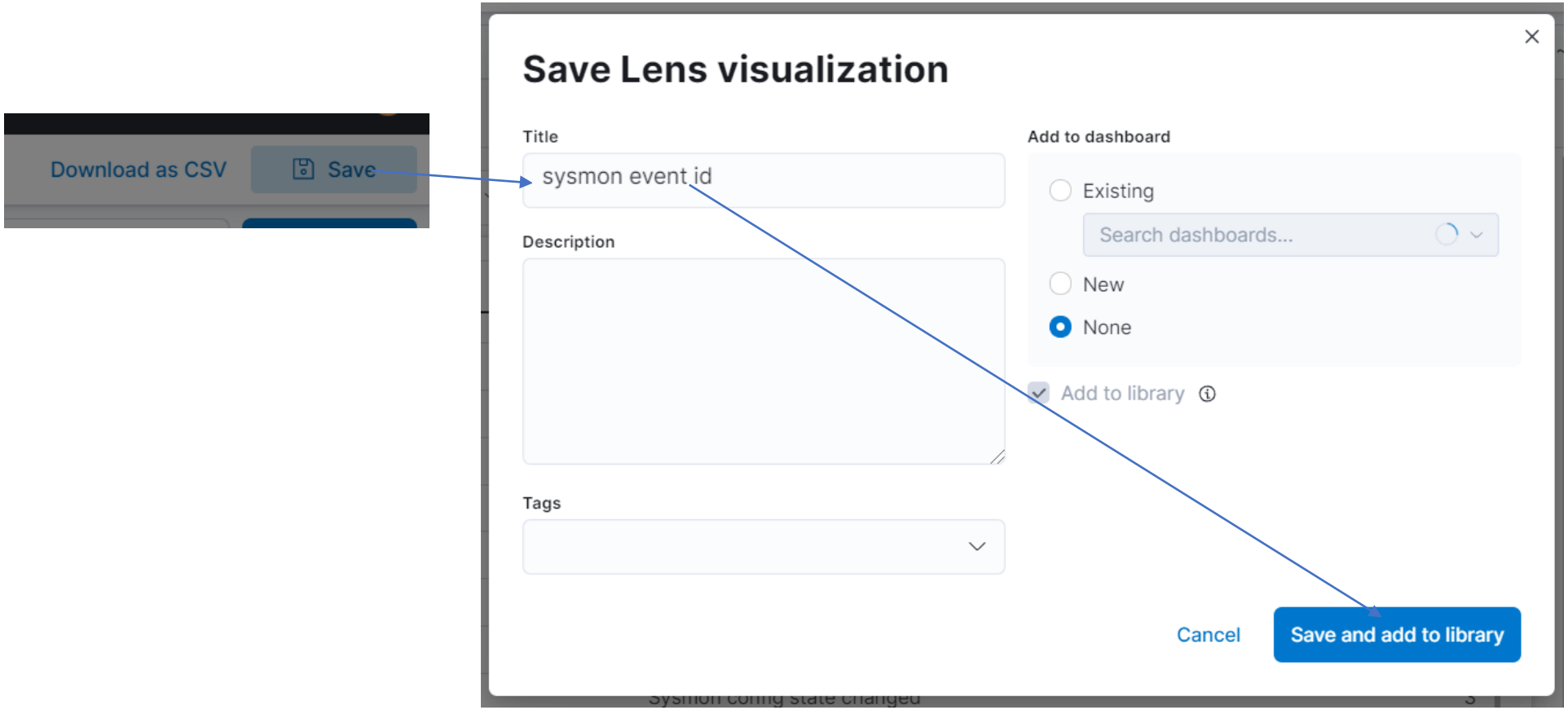


3. 테이블 구성요소를 다음과 같이 설정

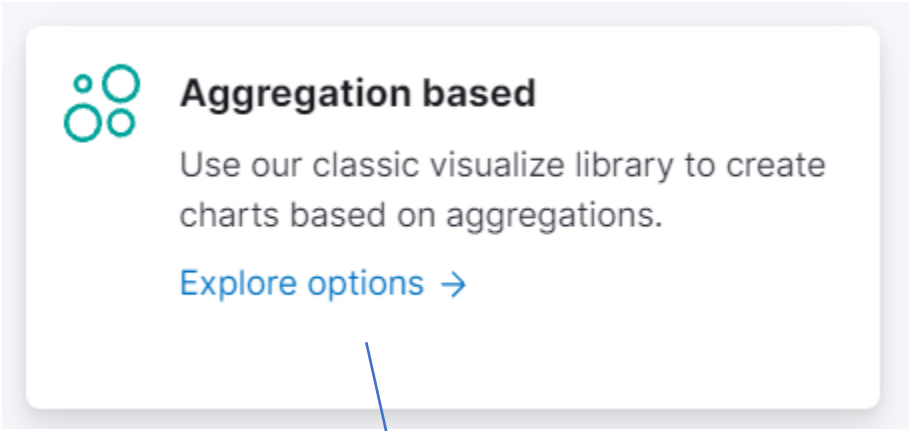
2. Visualize Library : 시각화 자료 만들기



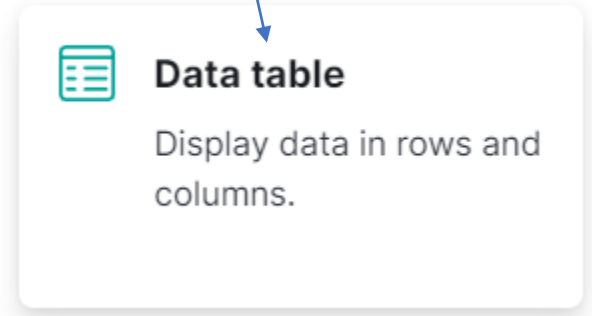
2. Visualize Library : 시각화 자료 만들기

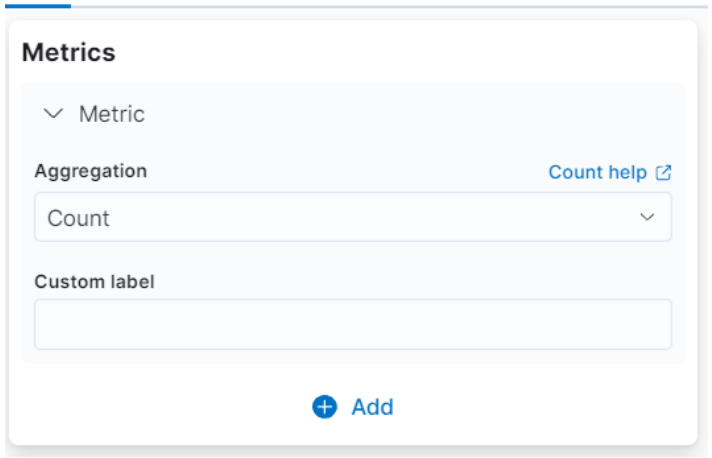


2. Visualize Library : 시각화 자료 만들기



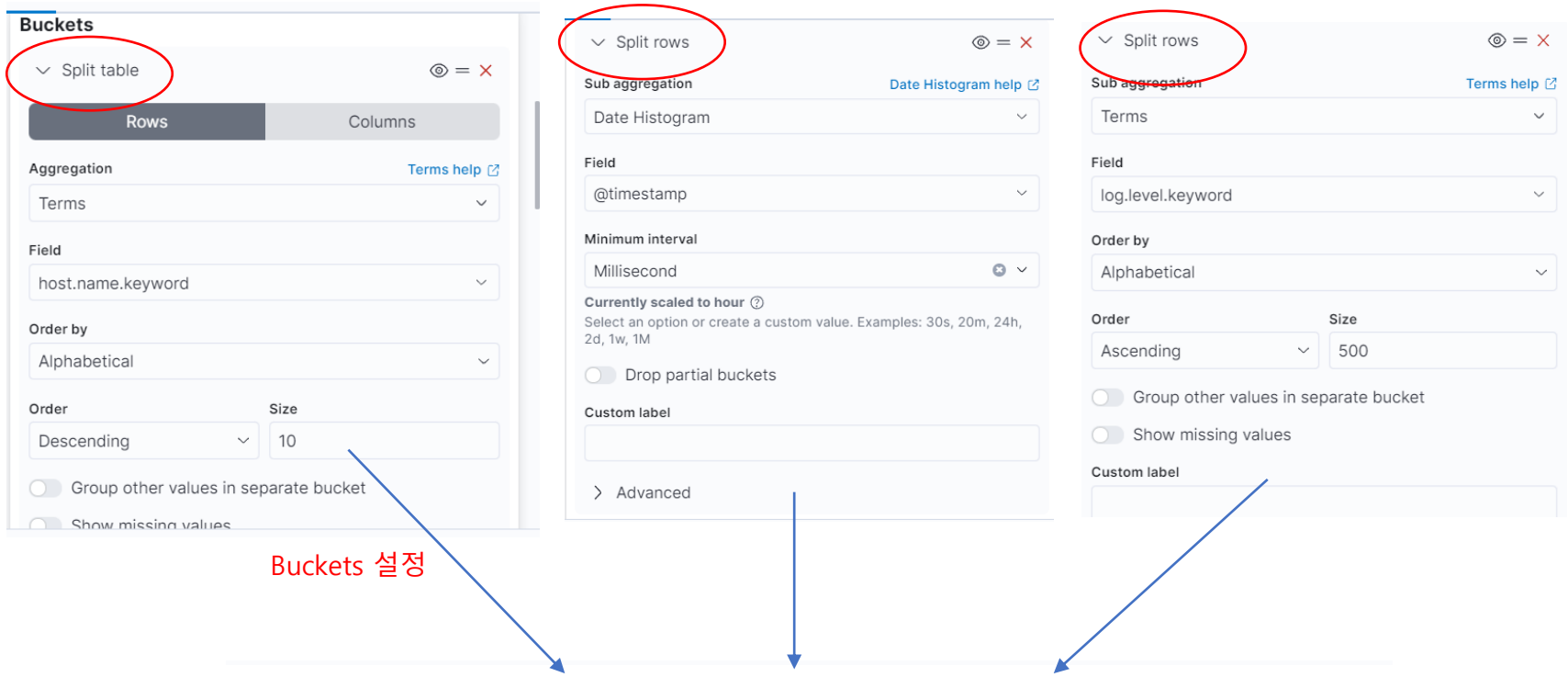
호스트별 정보 생성하기





Metrics 설정

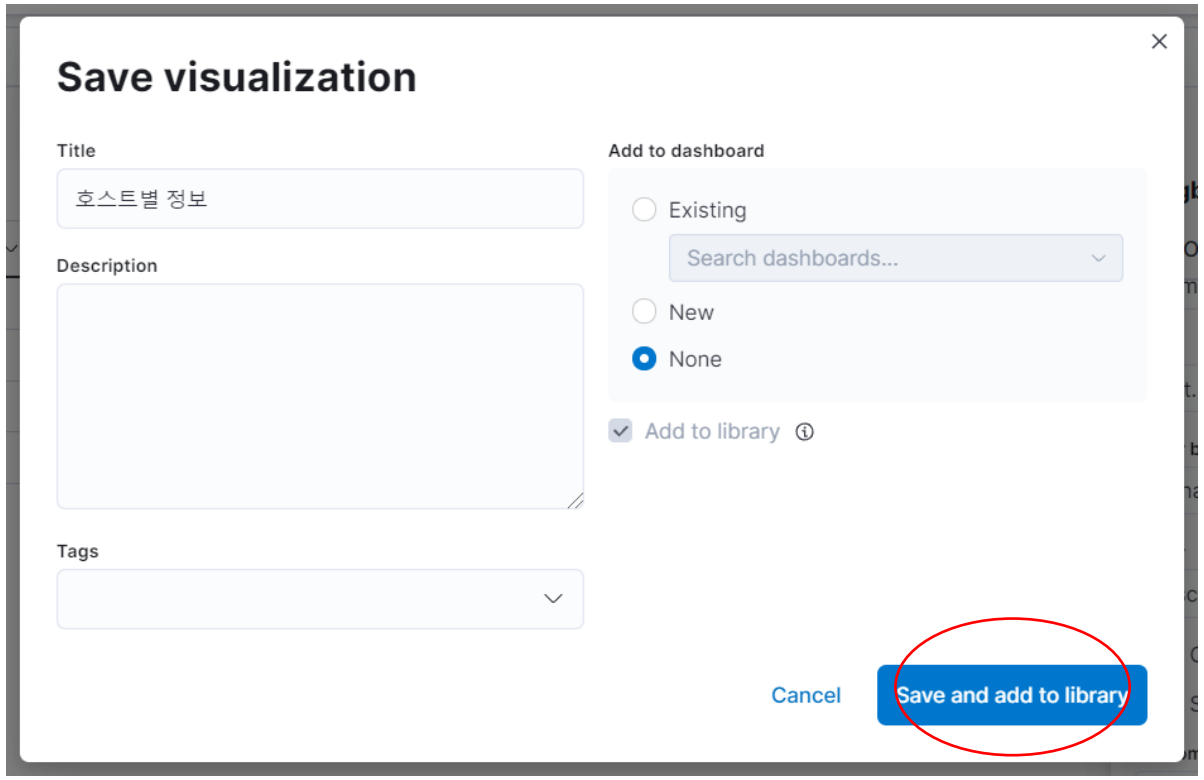
2. Visualize Library : 시각화 자료 만들기



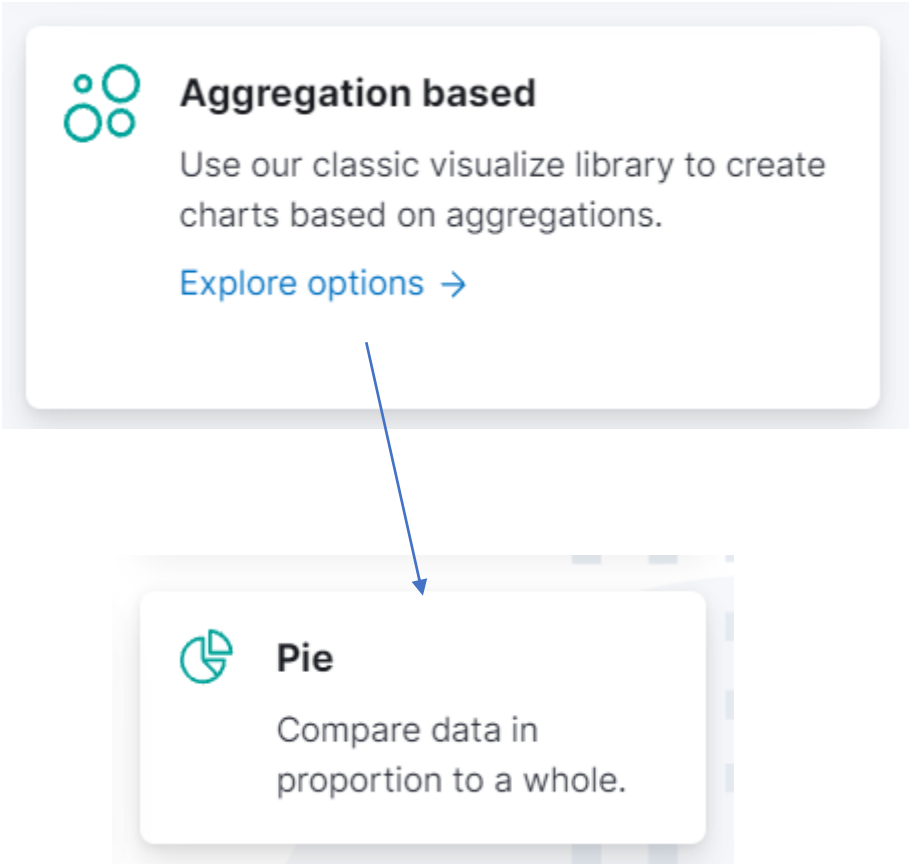
DESKTOP-1896AKK: host.name.keyword: Descending

@timestamp per hour	log.level.keyword: Ascending	Count
2021-10-08 03:00	오류	4
2021-10-08 03:00	정보	378
2021-10-09 20:00	정보	1,753
2021-10-09 21:00	정보	134

2. Visualize Library : 시각화 자료 만들기

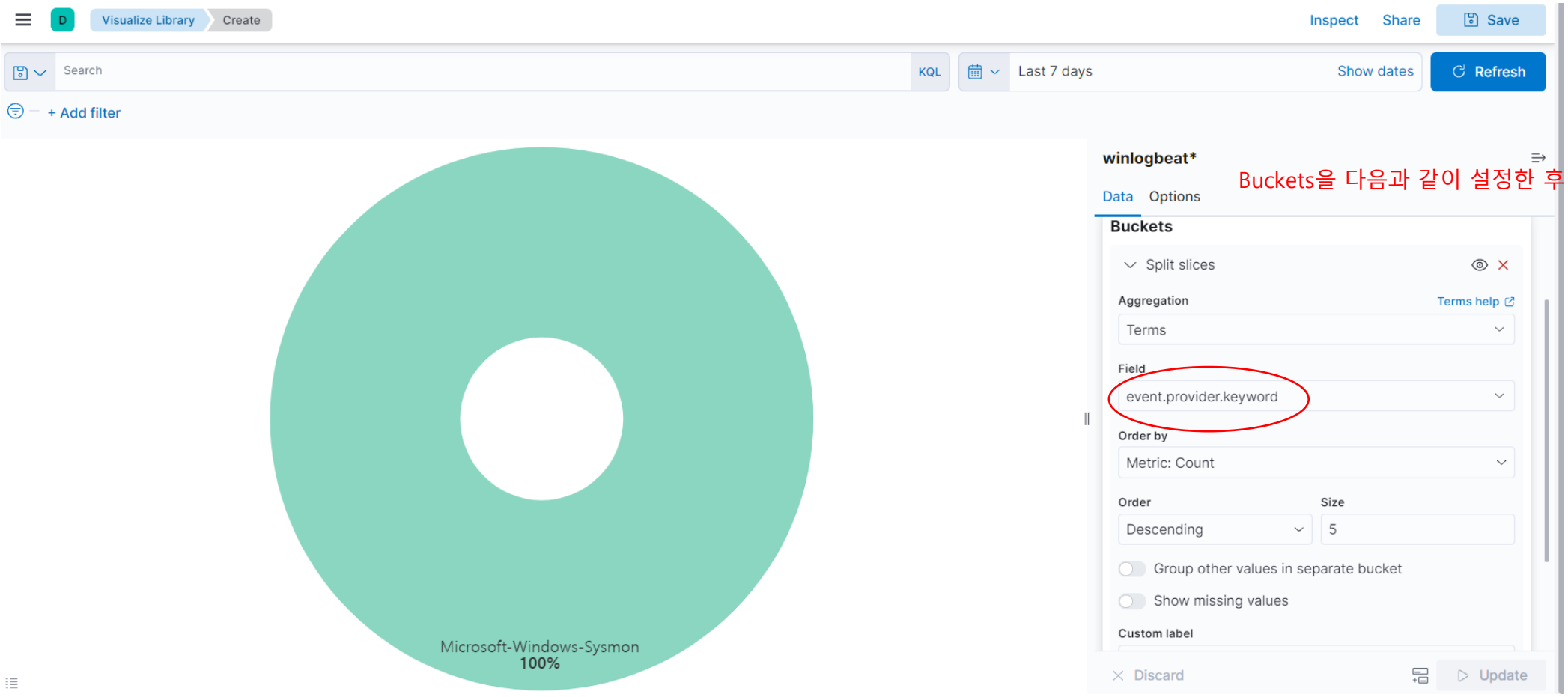


2. Visualize Library : 시각화 자료 만들기



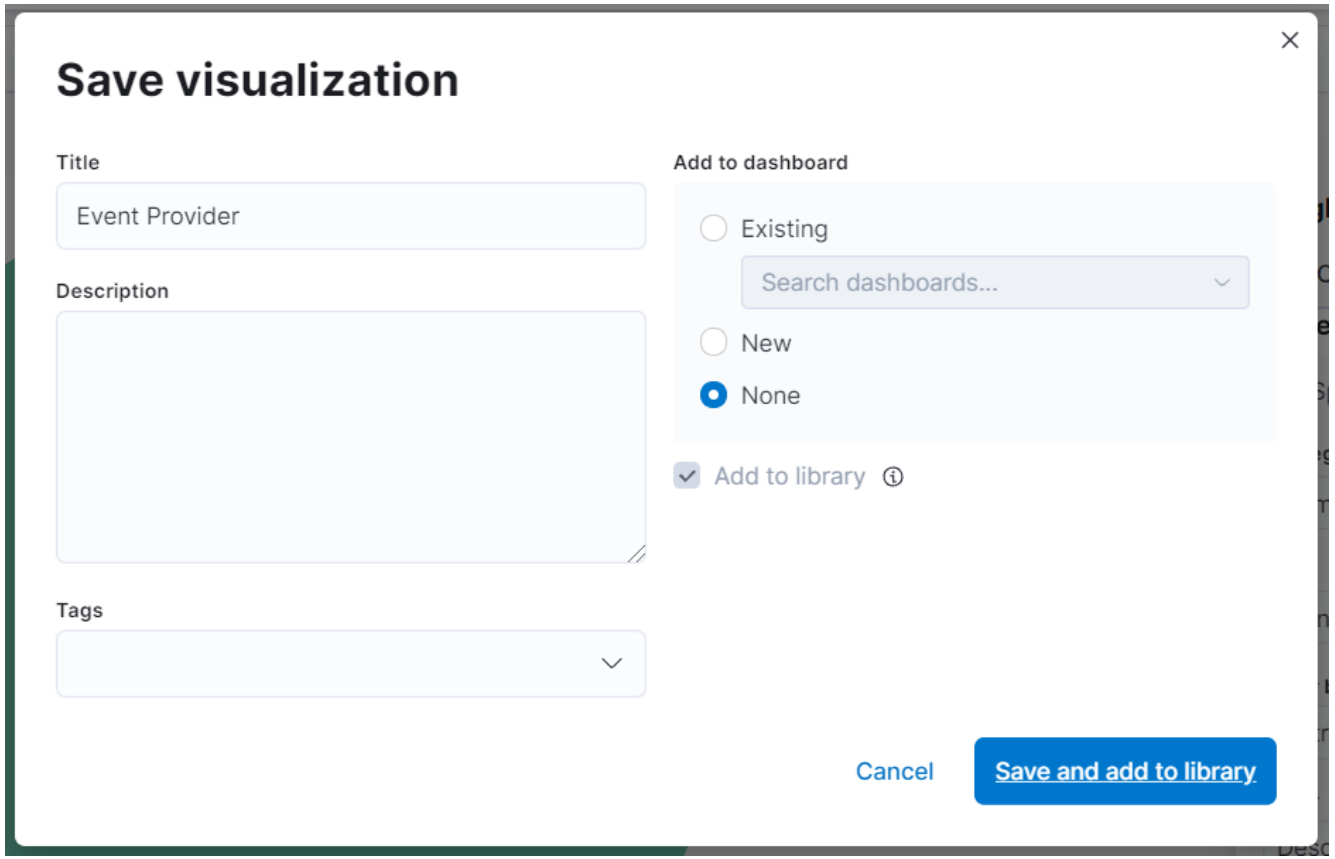
파이 차트 생성하기

2. Visualize Library : 시각화 자료 만들기

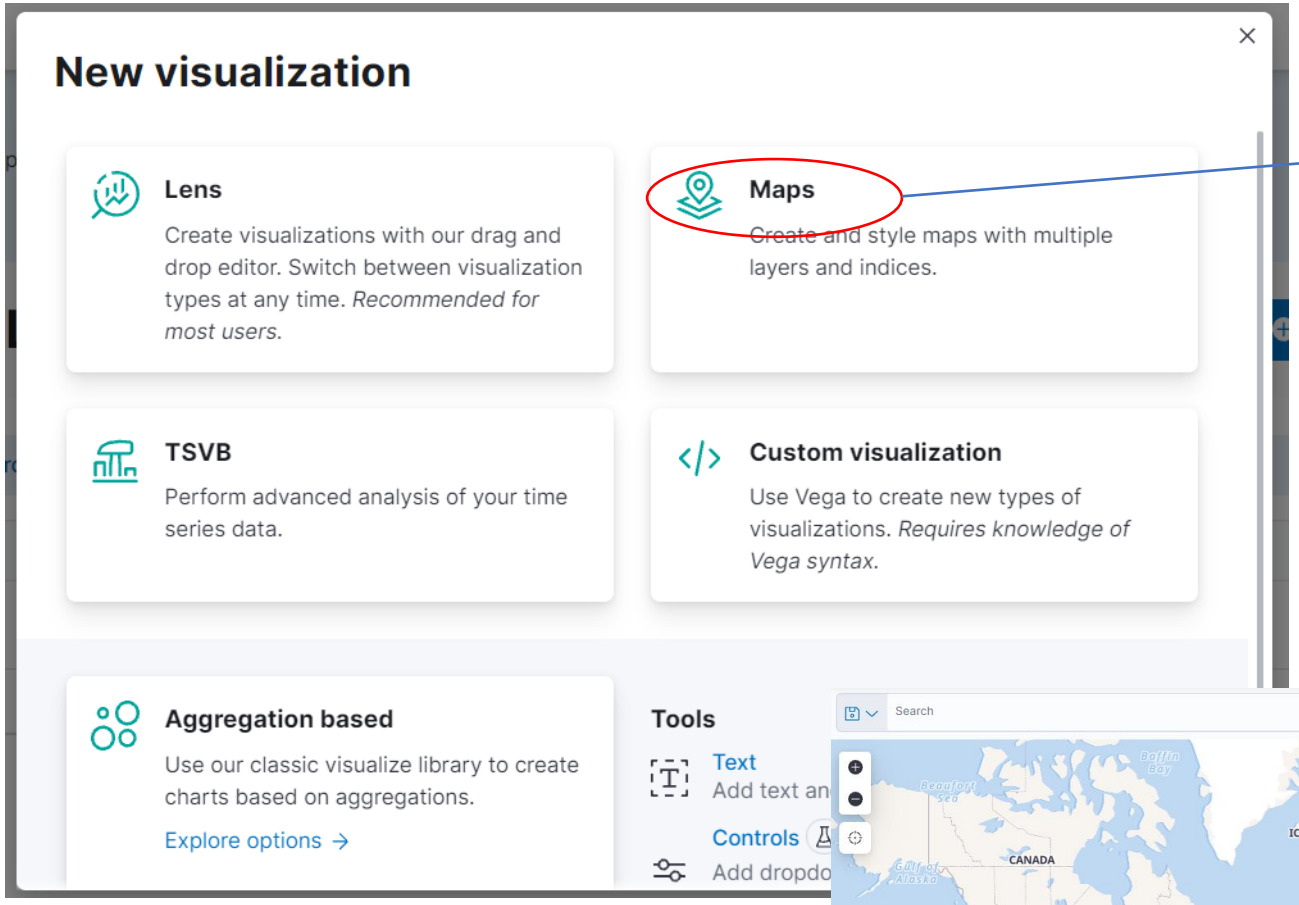


Buckets을 다음과 같이 설정한 후 save

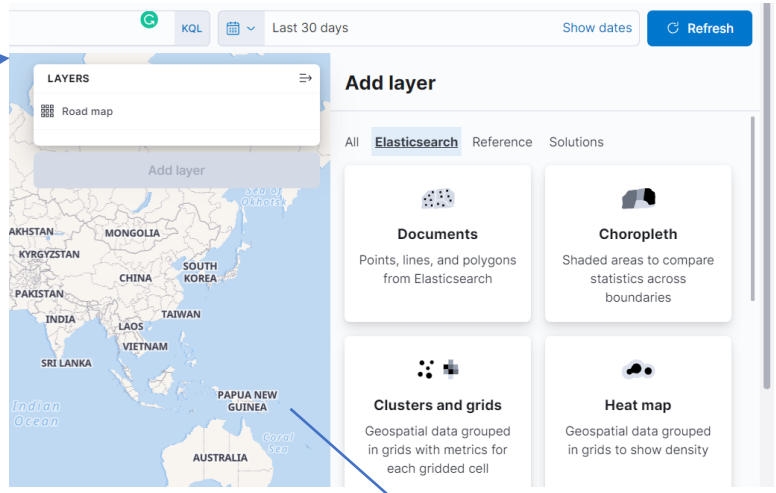
2. Visualize Library : 시각화 자료 만들기



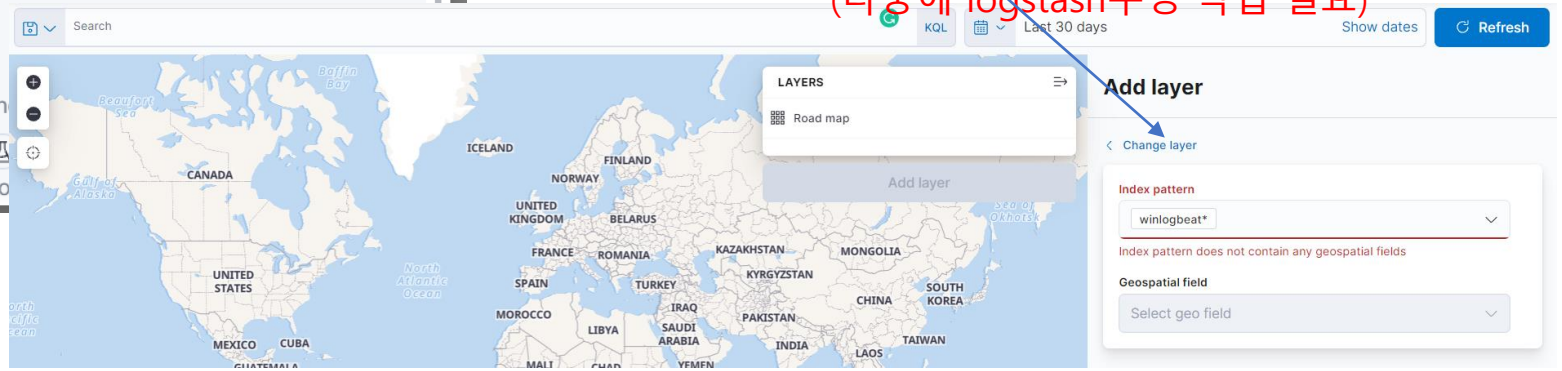
2. Visualize Library : 시각화 자료 만들기(보류)



Map



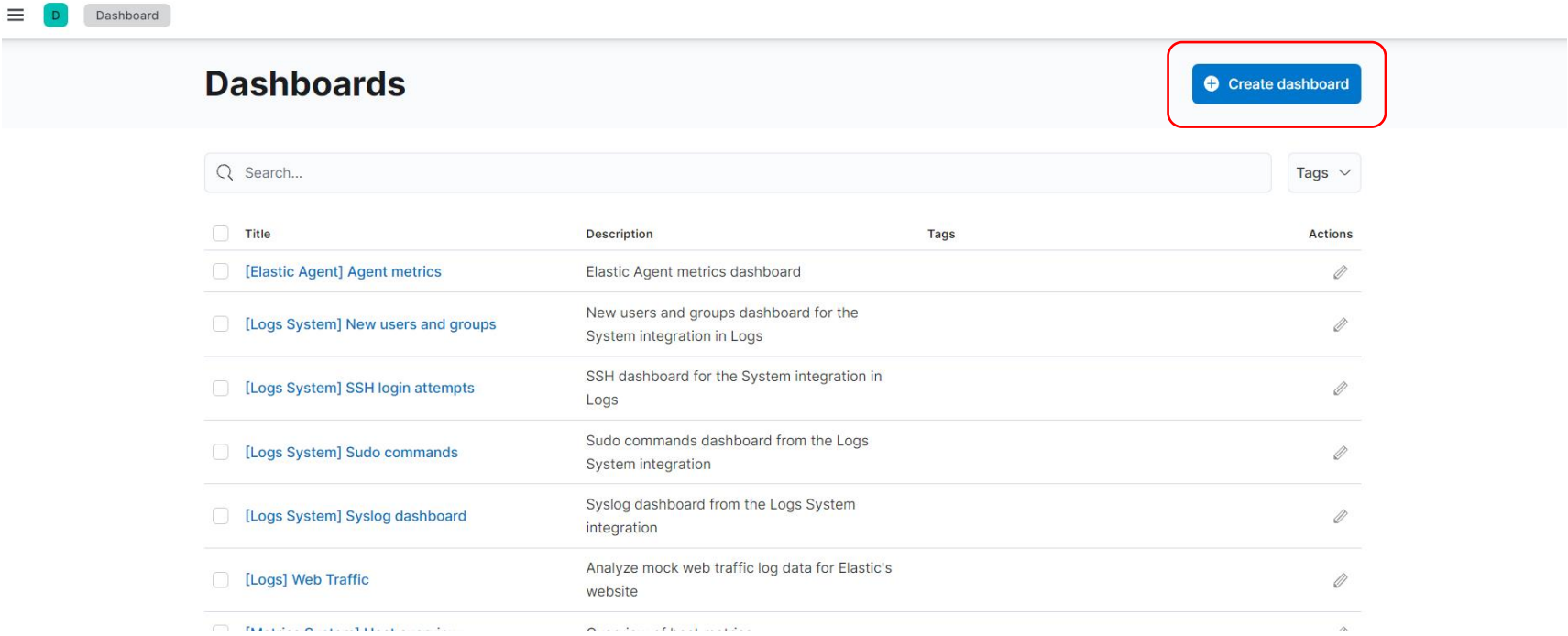
geo포인트가 있어야 함
(나중에 logstash수정 작업 필요)



3. Dashboard : 대시보드 생성

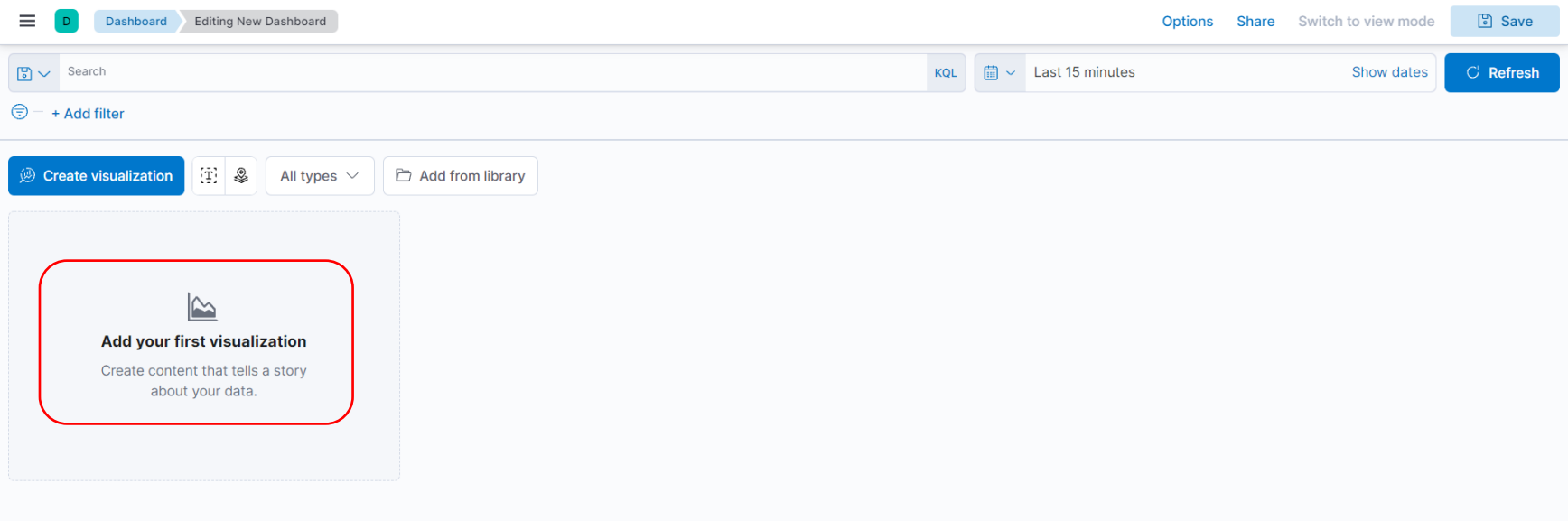
- Dashboard?
  - 데이터 실시간 관찰 및 검색 가능, 시각화된 자료들의 묶음
  - 한 화면 안에서 데이터를 여러 유형으로 표시하여 관찰할 수 있음

3. Dashboard : 대시보드 생성



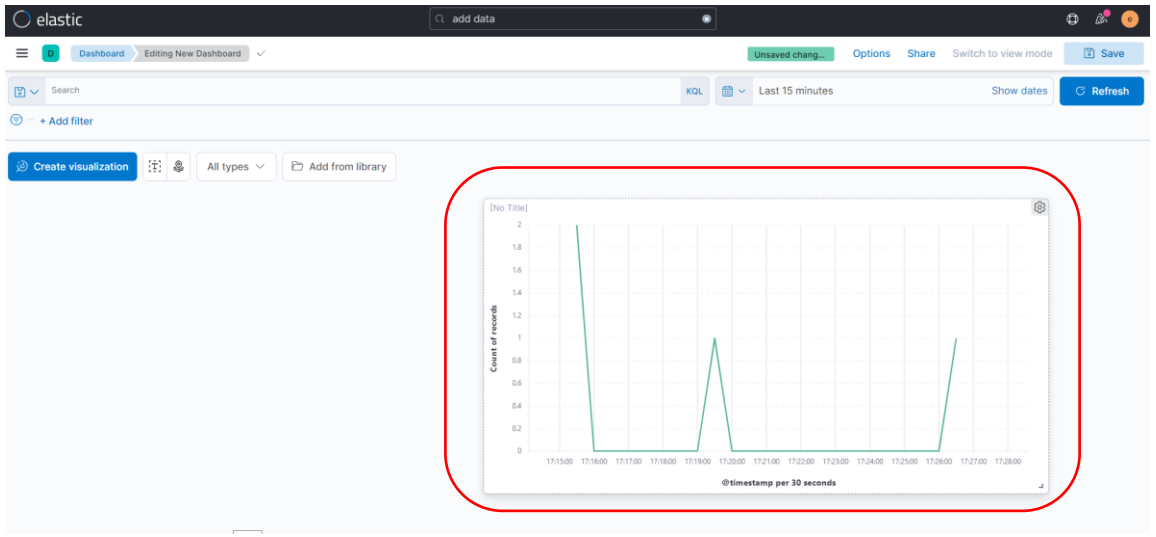
- 대시보드 탭으로 들어가 Create Dashboard

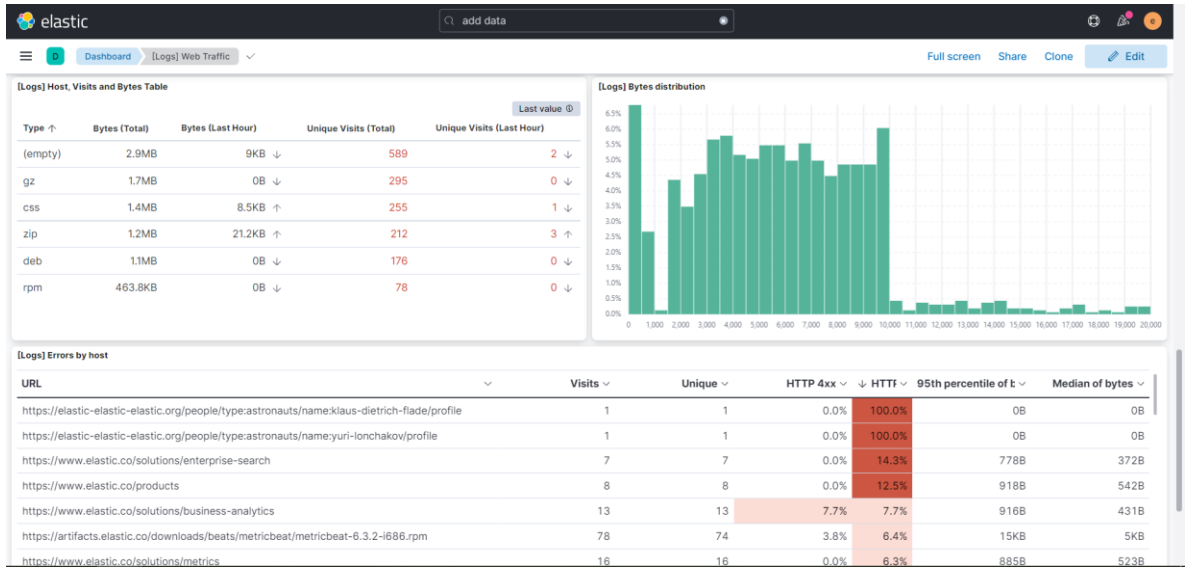
3. Dashboard : 대시보드 생성



- 대시보드를 사용하기 위해서는 Visualize에서 데이터 시각화 작업이 필요

3. Dashboard : 대시보드 생성 (예시)

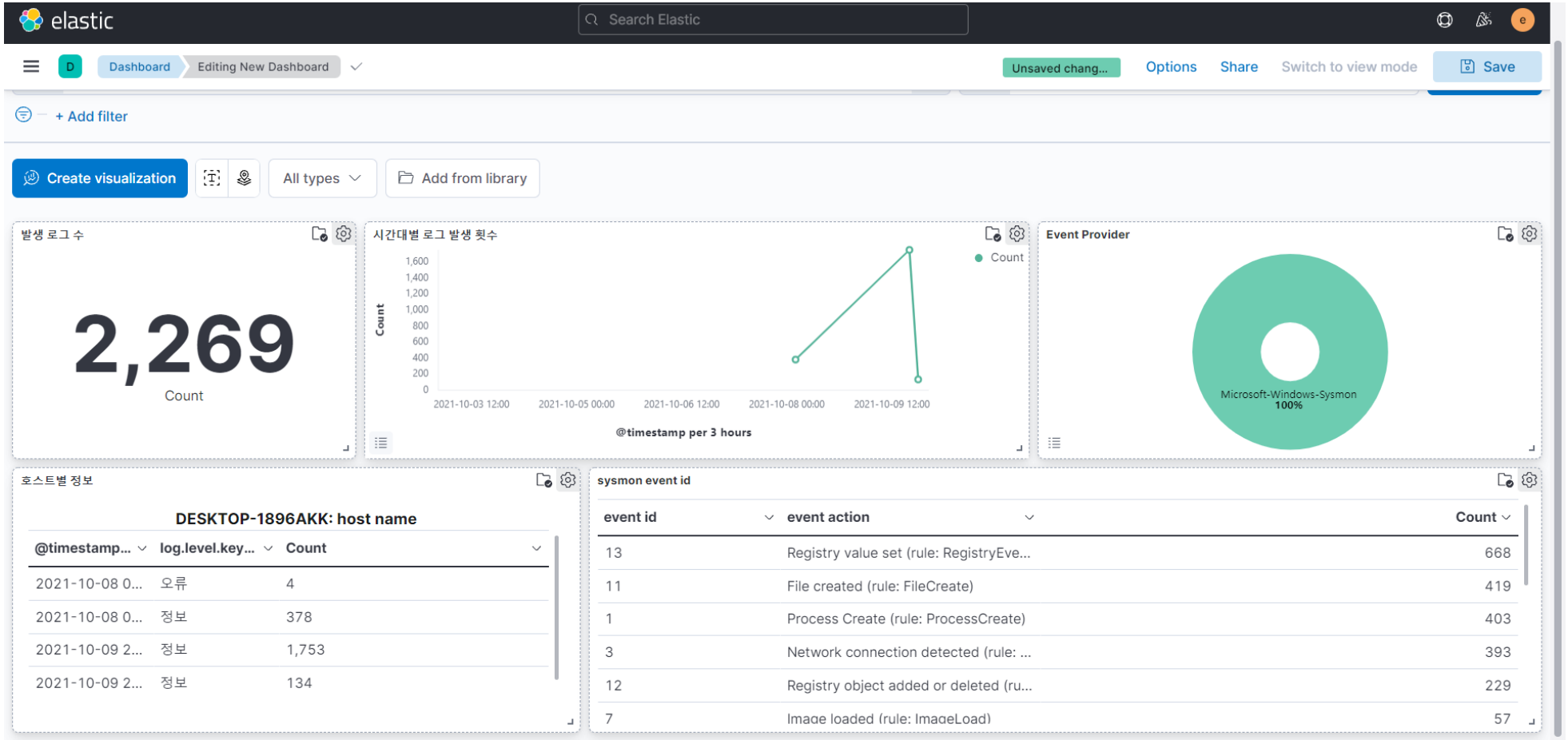




[샘플 데이터의 대시보드]

- Visualize된 자료를 원하는 위치로 끌어 직접 보기 편한 위치로 배치 가능
- 시각화된 여러 유형의 데이터들을 원하는 위치에 놓아 한눈에 볼 수 있음

3. Dashboard : 대시보드 생성



- 생성한 Visualization 자료를 가져와 만든 대시보드

3. Dashboard : 대시보드 생성

- log&악성 행위 수집을 위해 필요한 Dashboard 구성 요소는 아직 조사 예정
  - 로그 수집 후 우리가 Visualization 해야 할 것들..
  - 1. Number of Event -
  - 2. Event level
  - 3. host별 정보
  - …

참고

- https://www.itworld.co.kr/howto/136899
- https://www.elastic.co/kr/blog/importing-csv-and-log-data-into-elasticsearch-with-file-data-visualizer