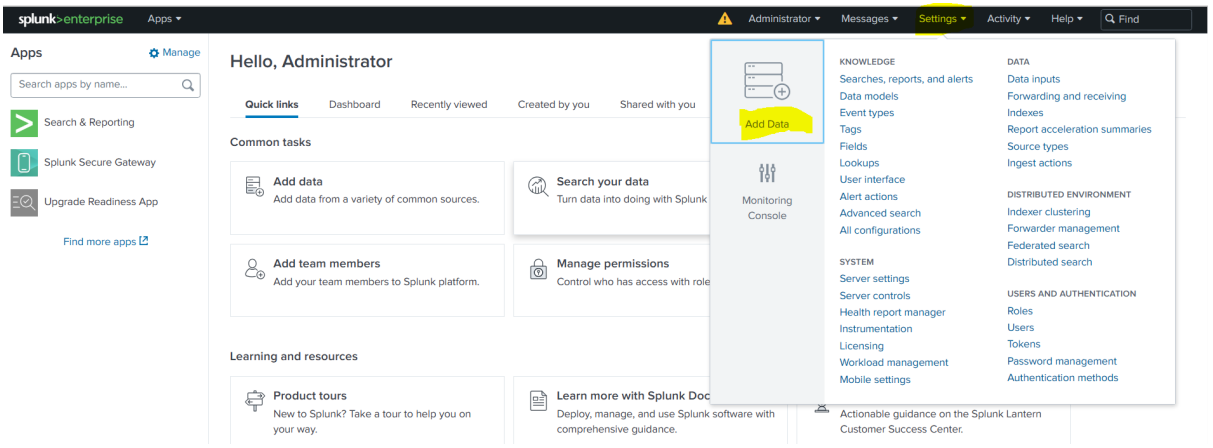
Guide for ingesting data.

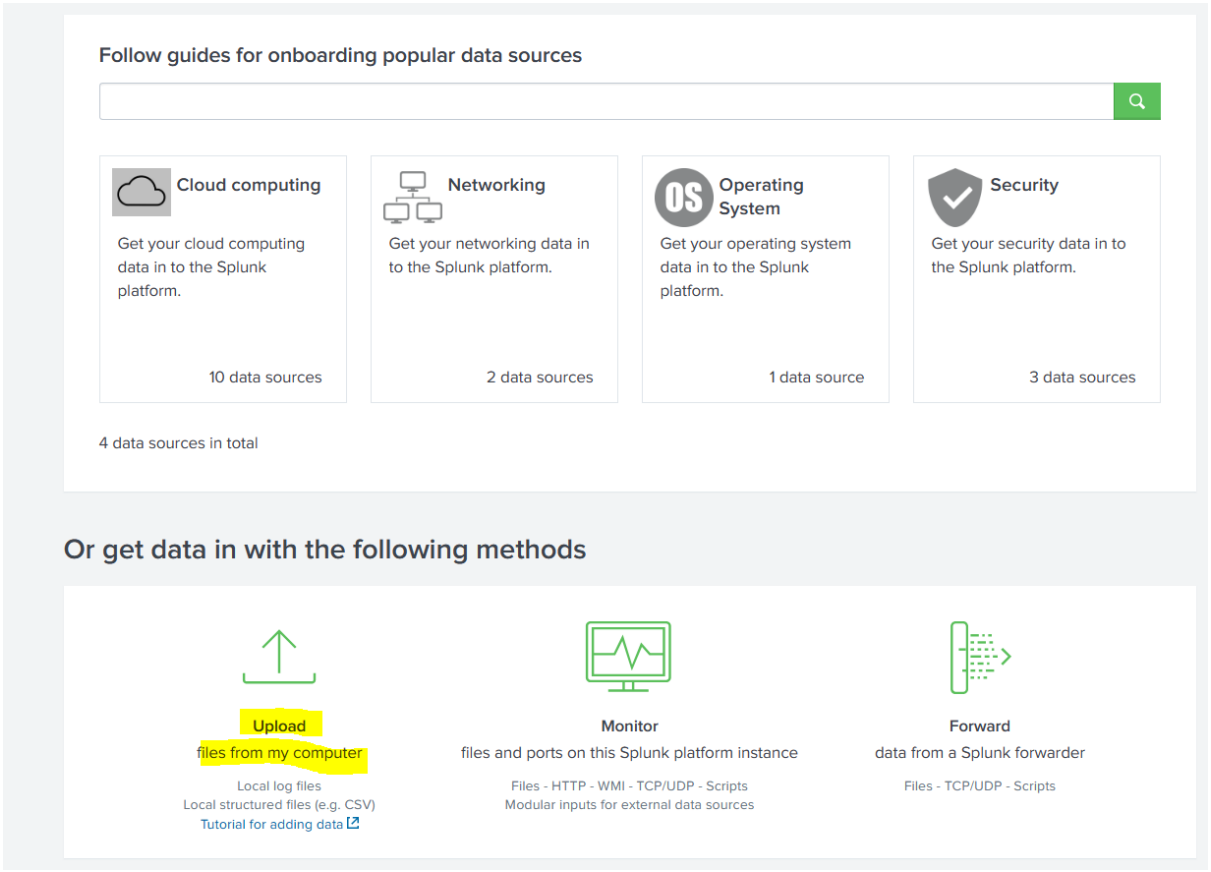
Draft event in json format:


```
{
    "publish_time": 1691770693.545, "data":
    {
        "insertId": "abcd8z4efgh4hijk", "jsonPayload":
        {
            "_eventId":"12345-21ad", "client":
            {
                "ip": "127.0.0.6", "port": 52847
            },
            "component": "OAuth", "eventName": "ACCESS-OUTCOME", "http":
            {
                "request":
                {
                    "headers":
                    {
                        "accept": ["application/json"], "host": ["authz-api.ew2.test01"], "user-agent": ["Java/11.0.15"], "x-forwarded-for": ["10.10.10.2"], "x-forwarded-proto": ["https"], "x-request-id": ["Test01-cyber01"]
                    },
                    "method": "GET", "path": "http://authz-api.ew2/cyber/root/abc_uri", "secure": false
                }
            },
            "level": "INFO", "realm": "/", "response":
            {
                "elapsedTime": 2, "elapsedTimeUnits": "MILLISECONDS", "status": "SUCCESSFUL", "statusCode": "200"
            },
            "source": "CyberEscape", "timestamp": "2023-08-11T16:18:10.630Z", "topic": "access", "transactionId": "12345-21ad-1234"
        },
        "labels":
        {
            "compute.googleapis.com/resource_name": "test01-CyberEscape01", "k8s-pod/app": "cyber", "k8s-pod/app_kubernetes_io/managed-by": "CyberEscape", "k8s-pod/app-kubernetes_io/name": "cyber",
            "K85-pod/pod-template-hash": "2c975b69ab", "k8s-pod/tier": "middle"
        },
        "logName": "projects/cyber01/logs/stdout", "receiveTimestamp": "2023-08-11T16: 18:13.2303788752", "resource":
            {
                "labels":
                {
                    "cluster_name": "test01-CyberEscape01-euwe2", "container_name": "opencyber", "location": "europe-west2", "pod_name": "cyber-1234cd", "project_id": "test01-CyberEscape01"
                },
                "type": "k8s_container"
            }, "severity": "INFO", "timestamp":"2023-08-11T16:18:10.6303514292"
    },
        "attributes":
        {
            "logging. googleapis.com/timestamp": "2023-08-11T16:18:10.630351429Z"
        }
}
```

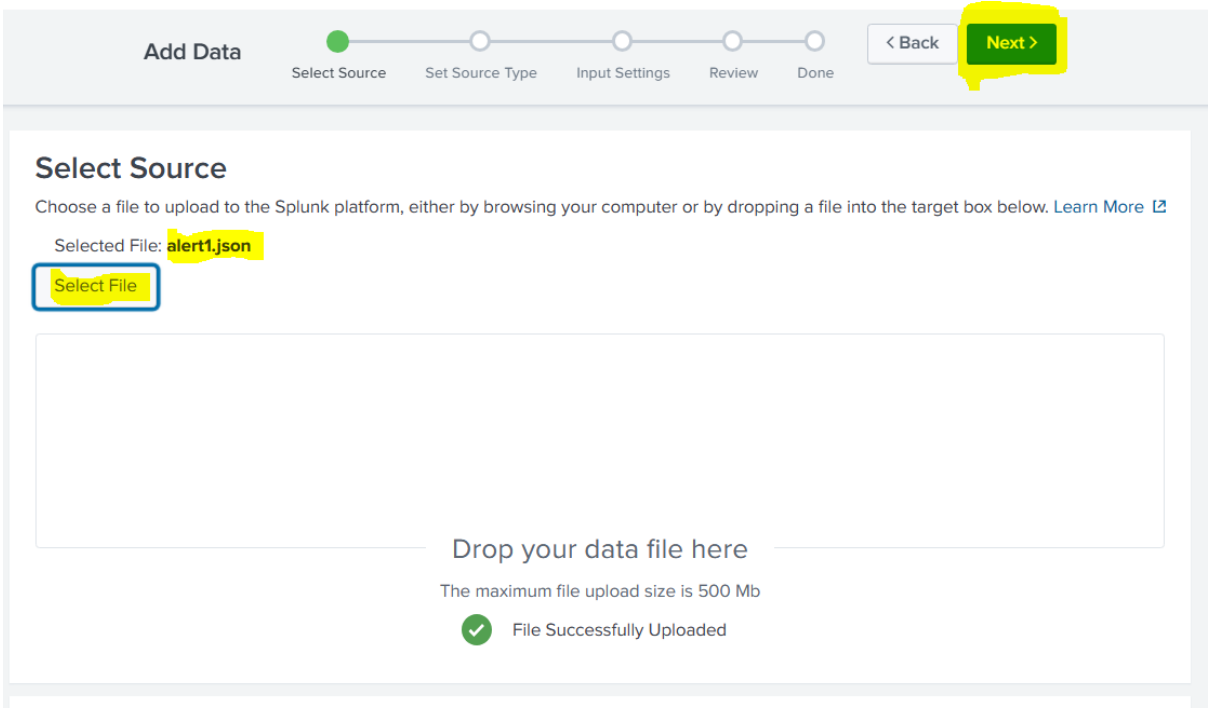

Settings > add data



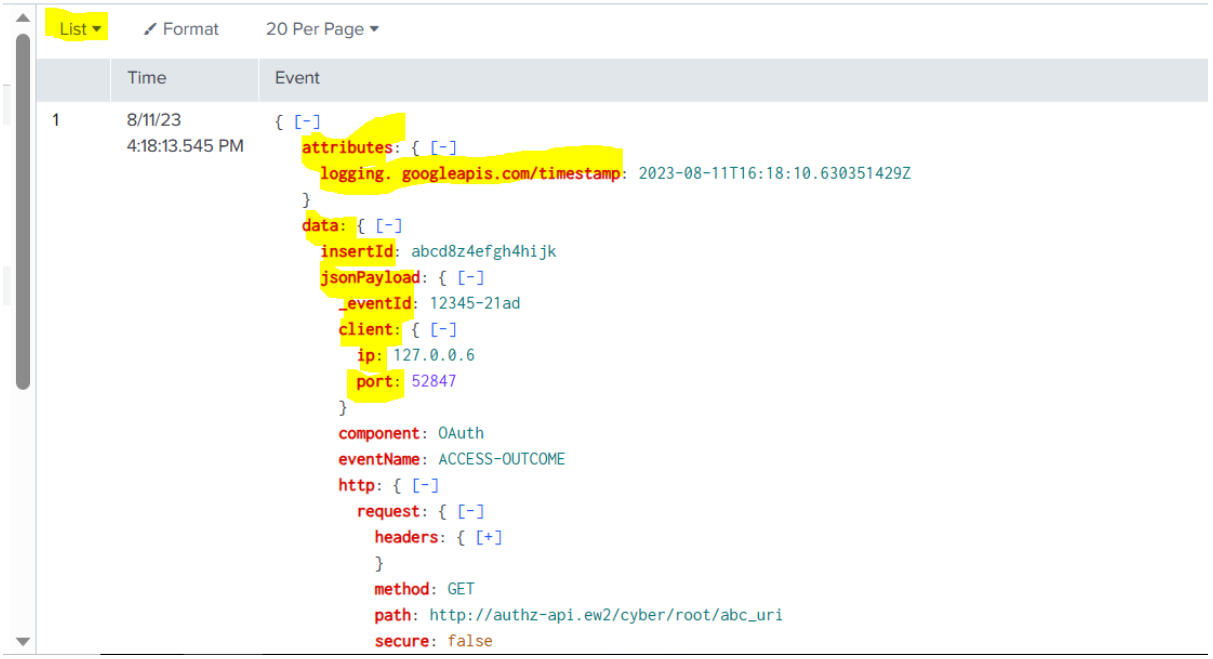
Click on ‘upload files from my computer’



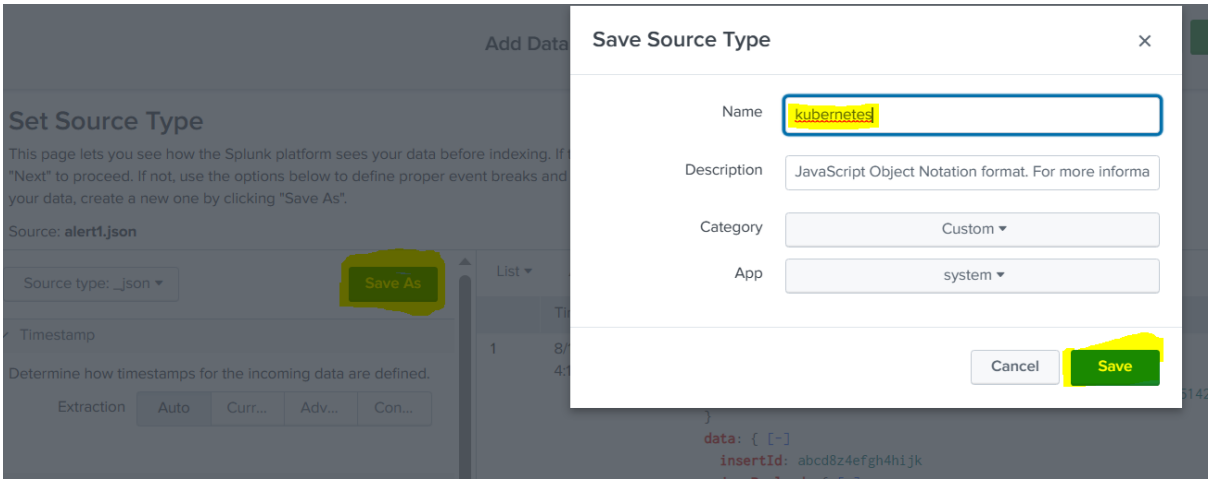
Select file > Next



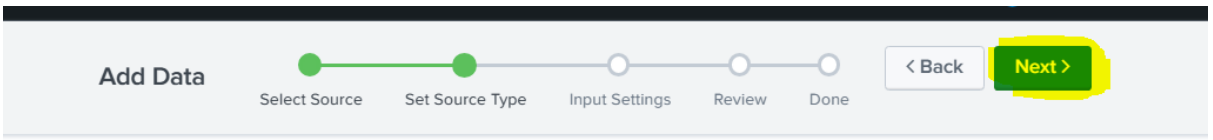
Check if the data is parsed properly



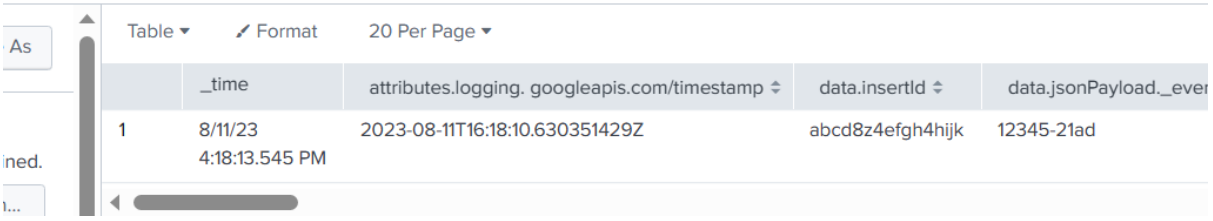
Set source type > save as > name:kubernetes > save



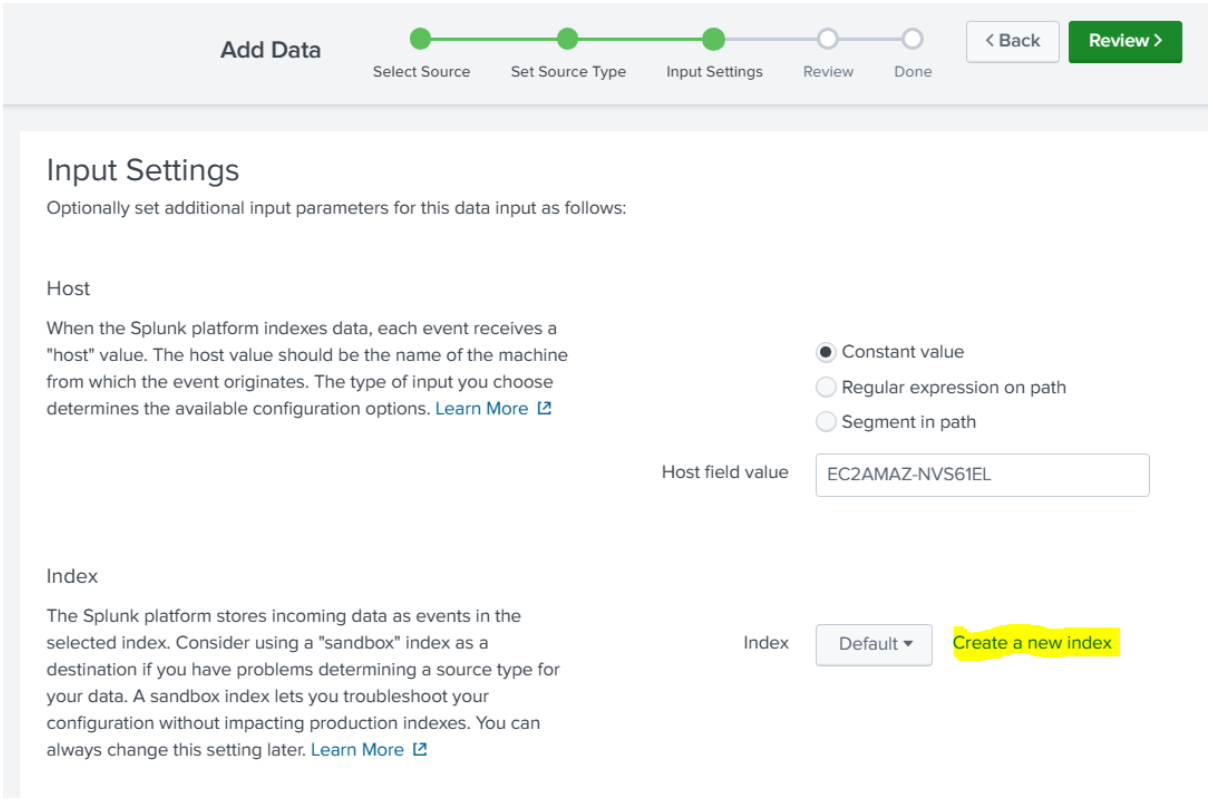
Click Next



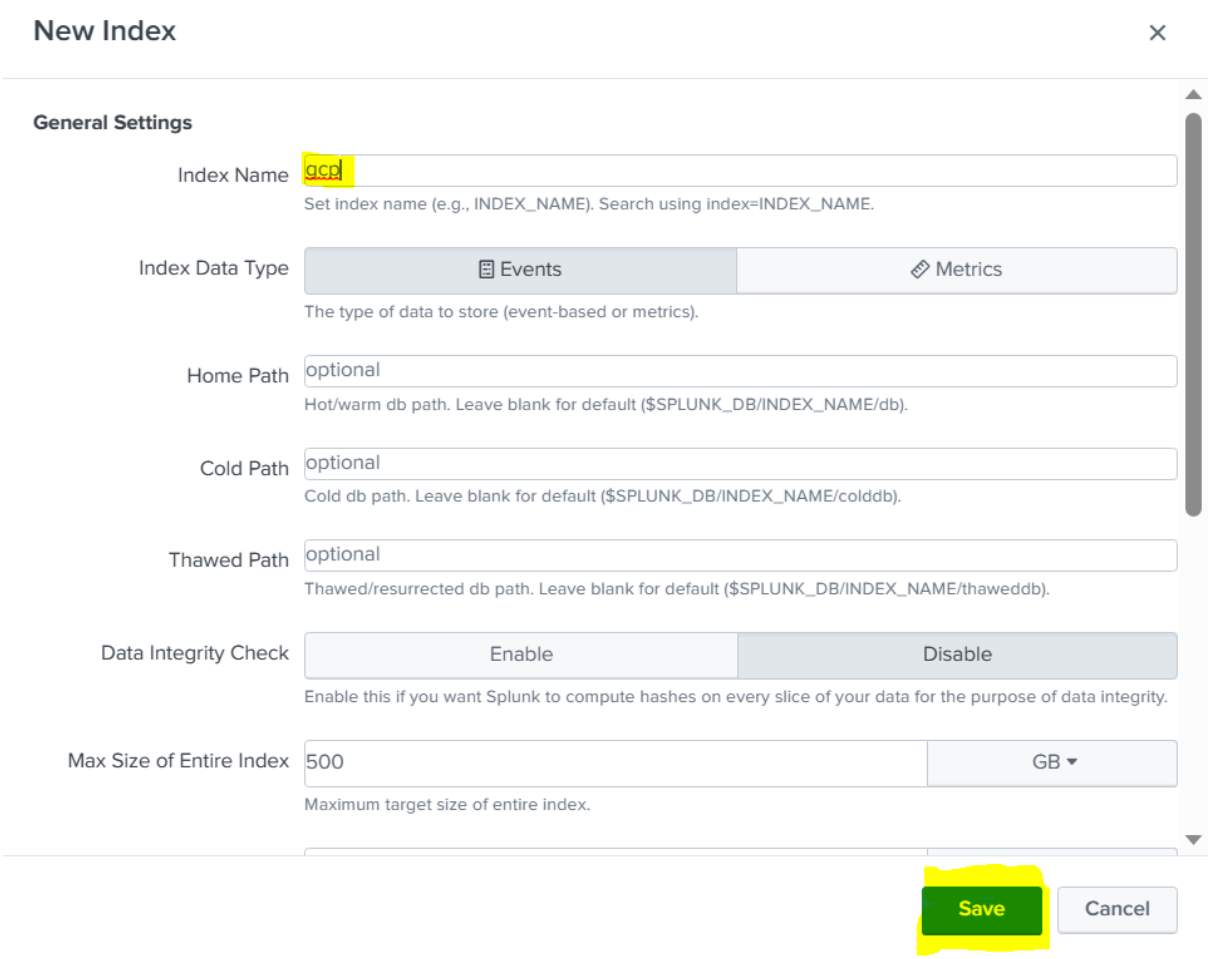
r data before indexing. If the events look correct and have the right timestamps, click
proper event breaks and timestamps. If you cannot find an appropriate source type for



If the index doesn't exist then create a new index

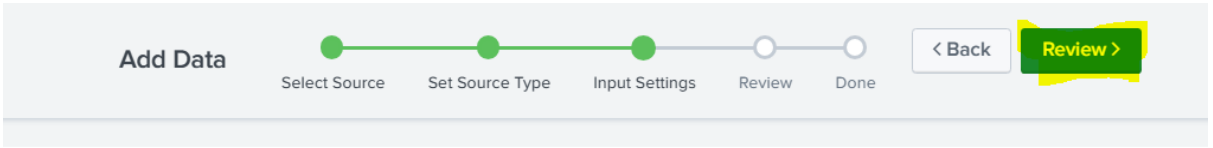


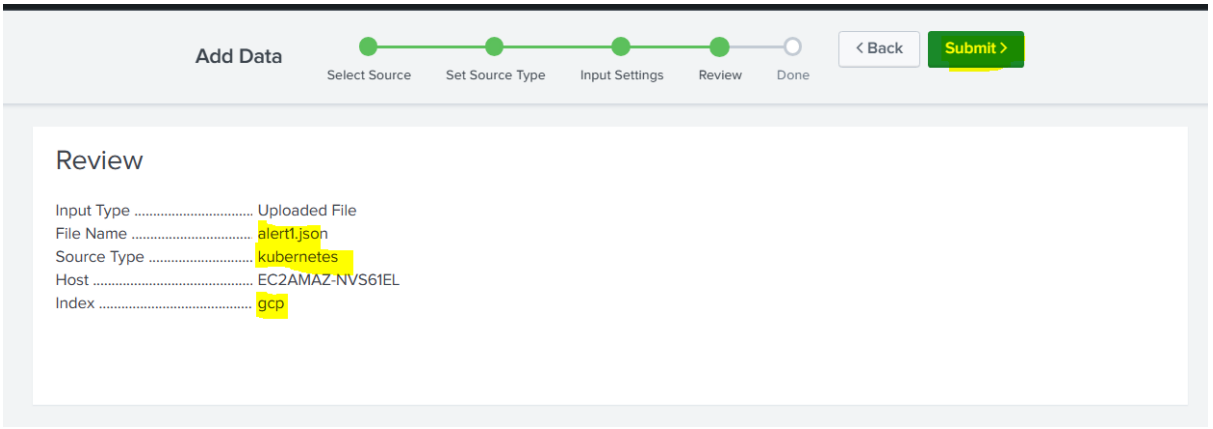
Name: gcp > save

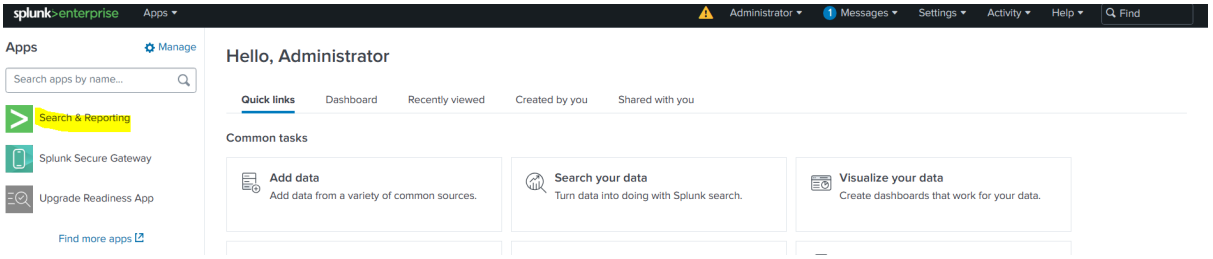


Click Review

Check all the fields and click Submit



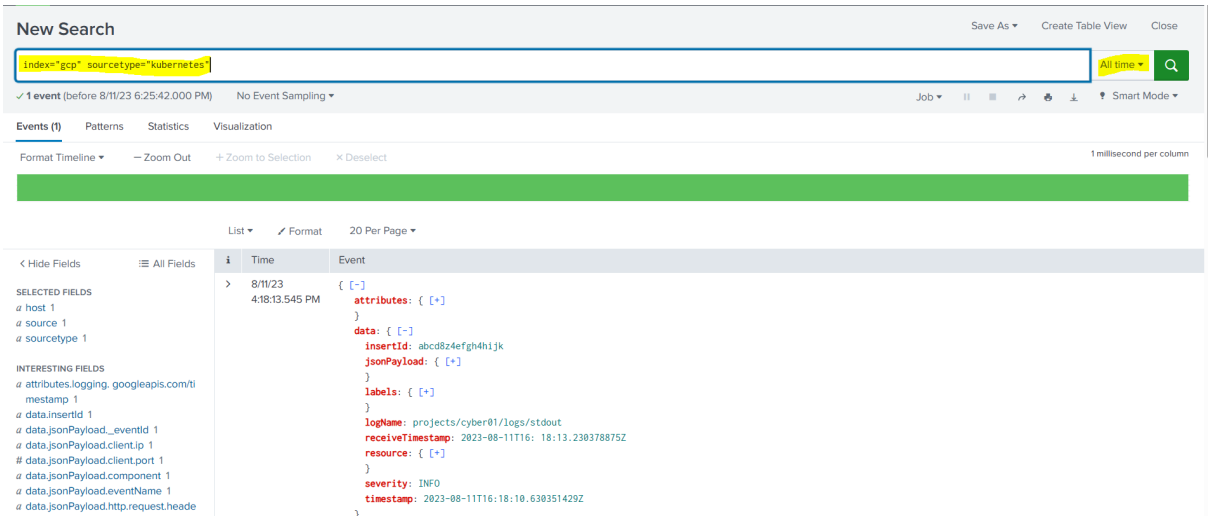




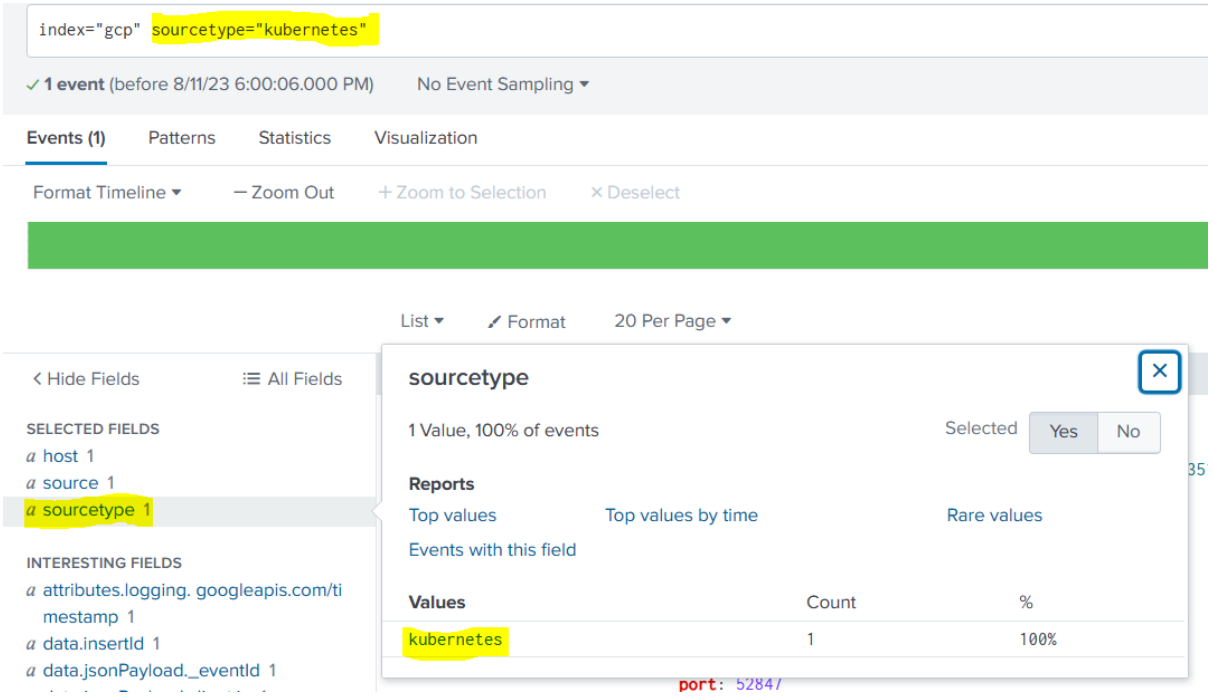
Go in the ‘Search & Reporting’ and type:

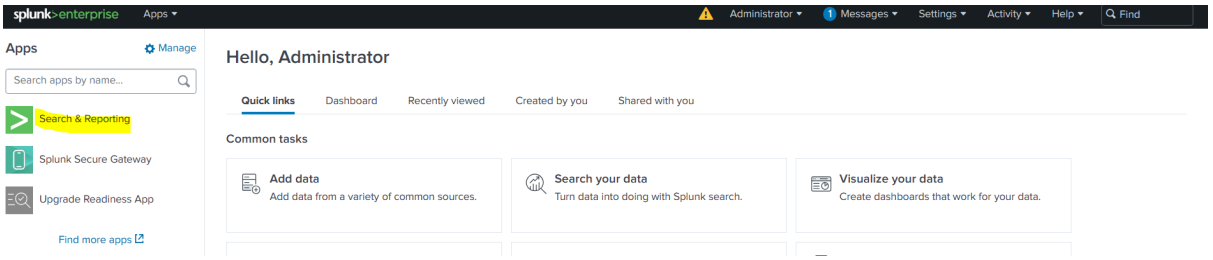
index="gcp" sourcetype="kubernetes"

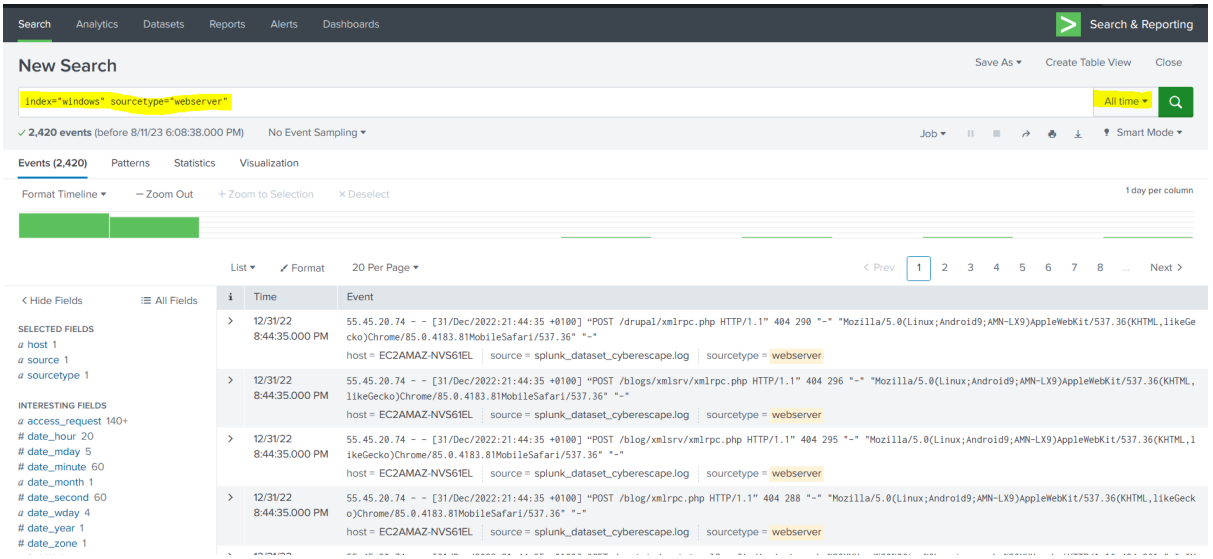
Time: all time

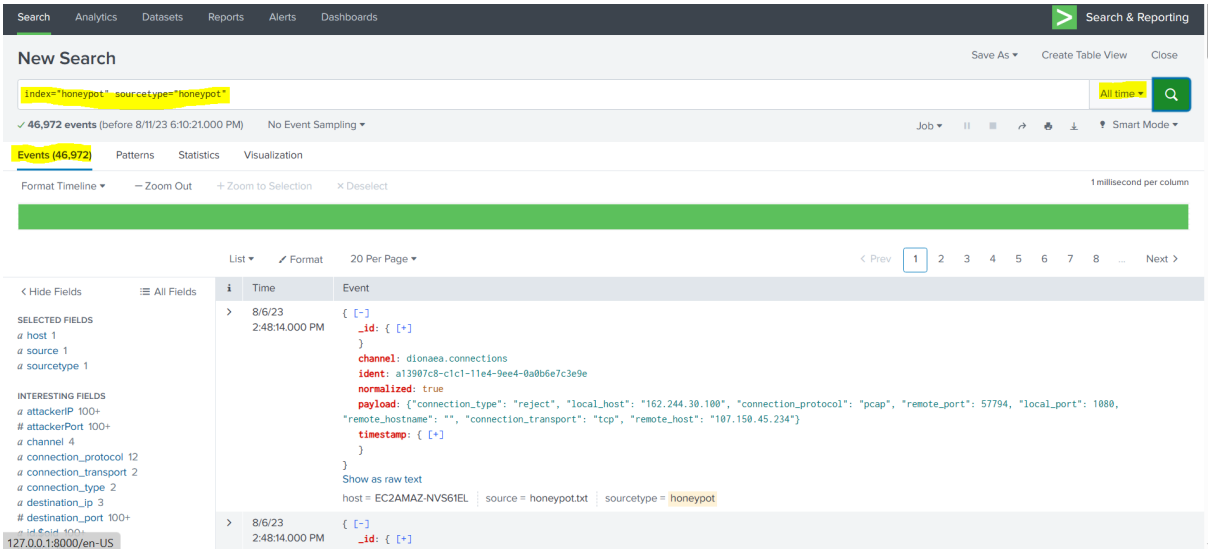


The fields are indexed on the left panel


index="gcp" sourcetype="kubernetes"
1 event (before 8/11/23 6:00:06.000 PM)
No Event Sampling
Events (1)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
List
Format
20 Per Page
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a attributes.logging. googleapis.com/timestamp 1
a data.insertId 1
a data.jsonPayload._eventId 1
sourcetype
1 Value, 100% of events
Selected
Yes
No
Reports
Top values
Top values by time
Rare values
Events with this field
Values
Count
%
kubernetes
1
100%
port: 52847


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Apps
Manage
Search apps by name...
Search & Reporting
Splunk Secure Gateway
Upgrade Readiness App
Find more apps
Hello, Administrator
Quick links
Dashboard
Recently viewed
Created by you
Shared with you
Common tasks
Add data
Add data from a variety of common sources.
Search your data
Turn data into doing with Splunk search.
Visualize your data
Create dashboards that work for your data.


Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
index="windows" sourcetype="webserver"
All time
2,420 events (before 8/11/23 6:08:38.000 PM)
No Event Sampling
Job
Smart Mode
Events (2,420)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 day per column
List
Format
20 Per Page
Prev
1
2
3
4
5
6
7
8
Next
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a access_request 140+
date_hour 20
date_mday 5
date_minute 60
a date_month 1
date_second 60
a date_wday 4
date_year 1
date_zone 1
Time
Event
12/31/22 8:44:35.000 PM
55.45.20.74 - - [31/Dec/2022:21:44:35 +0100] "POST /drupal/xmlrpc.php HTTP/1.1" 404 290 "-" "Mozilla/5.0(Linux;Android9;AMN-LX9)AppleWebKit/537.36(KHTML,likeGecko)Chrome/85.0.4183.81MobileSafari/537.36" "-"
host = EC2AMAZ-NVS61EL source = splunk_dataset_cyberescape.log sourcetype = webserver
12/31/22 8:44:35.000 PM
55.45.20.74 - - [31/Dec/2022:21:44:35 +0100] "POST /blogs/xmlsrv/xmlrpc.php HTTP/1.1" 404 296 "-" "Mozilla/5.0(Linux;Android9;AMN-LX9)AppleWebKit/537.36(KHTML,likeGecko)Chrome/85.0.4183.81MobileSafari/537.36" "-"
host = EC2AMAZ-NVS61EL source = splunk_dataset_cyberescape.log sourcetype = webserver
12/31/22 8:44:35.000 PM
55.45.20.74 - - [31/Dec/2022:21:44:35 +0100] "POST /blog/xmlsrv/xmlrpc.php HTTP/1.1" 404 295 "-" "Mozilla/5.0(Linux;Android9;AMN-LX9)AppleWebKit/537.36(KHTML,likeGecko)Chrome/85.0.4183.81MobileSafari/537.36" "-"
host = EC2AMAZ-NVS61EL source = splunk_dataset_cyberescape.log sourcetype = webserver
12/31/22 8:44:35.000 PM
55.45.20.74 - - [31/Dec/2022:21:44:35 +0100] "POST /blog/xmlrpc.php HTTP/1.1" 404 288 "-" "Mozilla/5.0(Linux;Android9;AMN-LX9)AppleWebKit/537.36(KHTML,likeGecko)Chrome/85.0.4183.81MobileSafari/537.36" "-"
host = EC2AMAZ-NVS61EL source = splunk_dataset_cyberescape.log sourcetype = webserver


Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
index="honeypot" sourcetype="honeypot"
All time
46,972 events (before 8/11/23 6:10:21.000 PM)
No Event Sampling
Job
Smart Mode
Events (46,972)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 millisecond per column
List
Format
20 Per Page
Prev
1
2
3
4
5
6
7
8
Next
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a attackerIP 100+
attackerPort 100+
a channel 4
a connection_protocol 12
a connection_transport 2
a connection_type 2
a destination_ip 3
destination_port 100+
Time
Event
8/6/23 2:48:14.000 PM
{ [-]
_id: { [+]
}
channel: dionaea.connections
ident: a13907c8-c1c1-11e4-9ee4-0a0b6e7c3e9e
normalized: true
payload: {"connection_type": "reject", "local_host": "162.244.30.100", "connection_protocol": "pcap", "remote_port": 57794, "local_port": 1080, "remote_hostname": "", "connection_transport": "tcp", "remote_host": "107.150.45.234"}
timestamp: { [+]
}
}
Show as raw text
host = EC2AMAZ-NVS61EL source = honeypot.txt sourcetype = honeypot
8/6/23 2:48:14.000 PM
{ [-]
_id: { [+]
127.0.0.1:8000/en-US