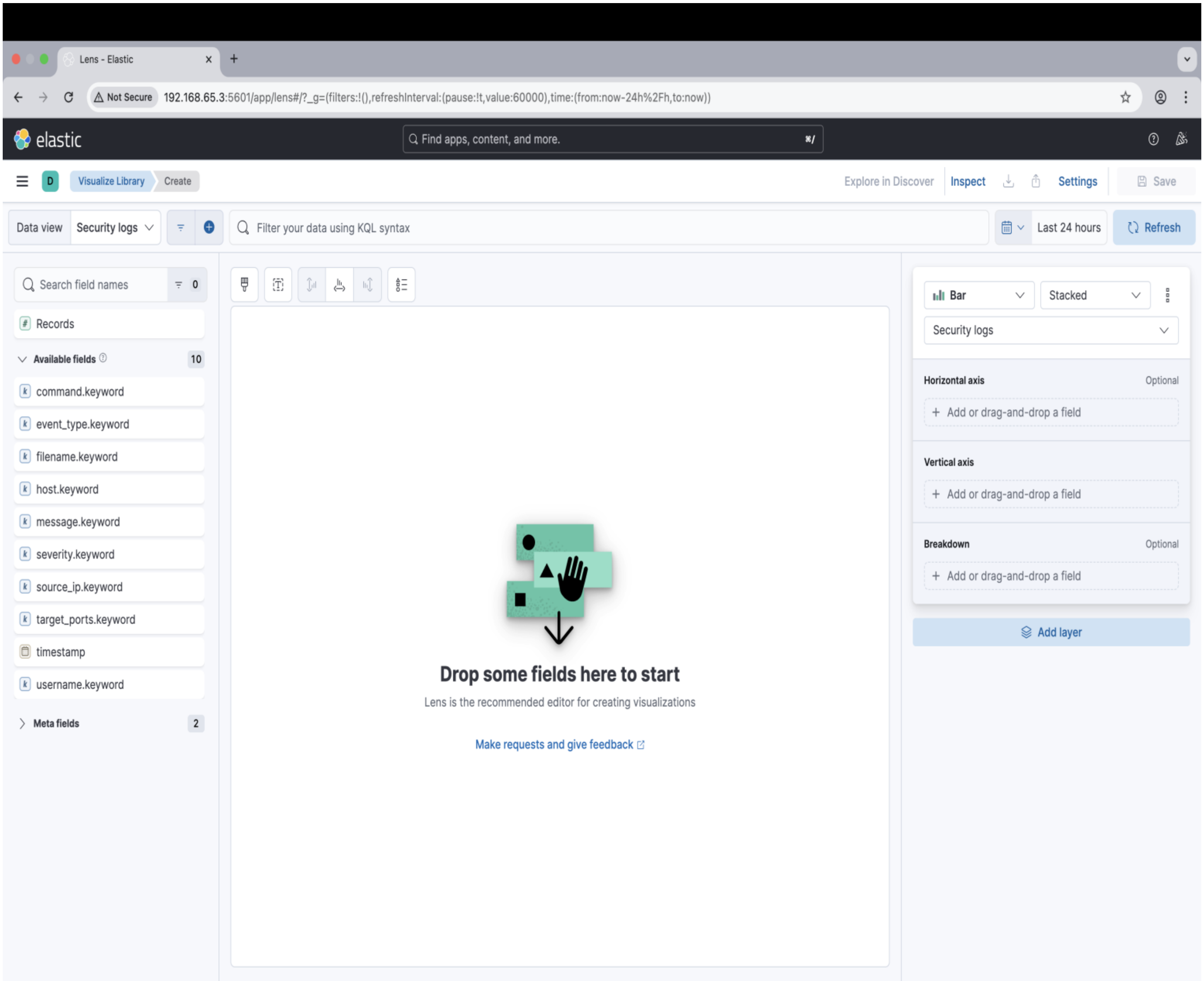
Screenshots

1. 8 security events



192.168.65.3:5601/app/lens#/?_g=(filters:!(),refreshInterval:(pause:!t,value:60000),time:(from:now-24h%2Fh,to:now))

Data view: Security logs

Last 24 hours

Available fields 10

- command.keyword
- event_type.keyword
- filename.keyword
- host.keyword
- message.keyword
- severity.keyword
- source_ip.keyword
- target_ports.keyword
- timestamp
- username.keyword

Meta fields 2

Bar · Stacked · Security logs

Horizontal axis (Optional): Add or drag-and-drop a field

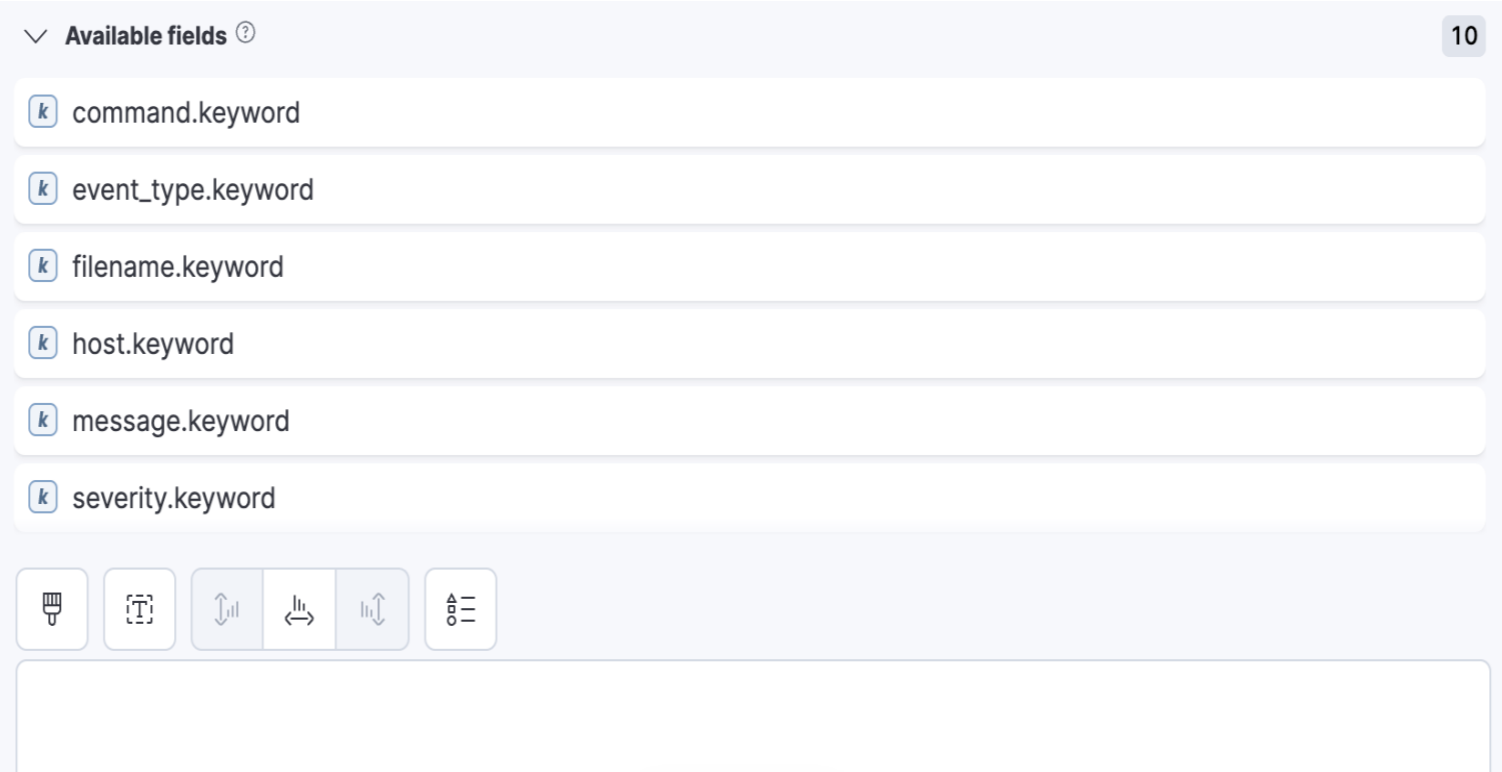
Vertical axis: Add or drag-and-drop a field

Breakdown (Optional): Add or drag-and-drop a field

Drop some fields here to start

Lens is the recommended editor for creating visualizations

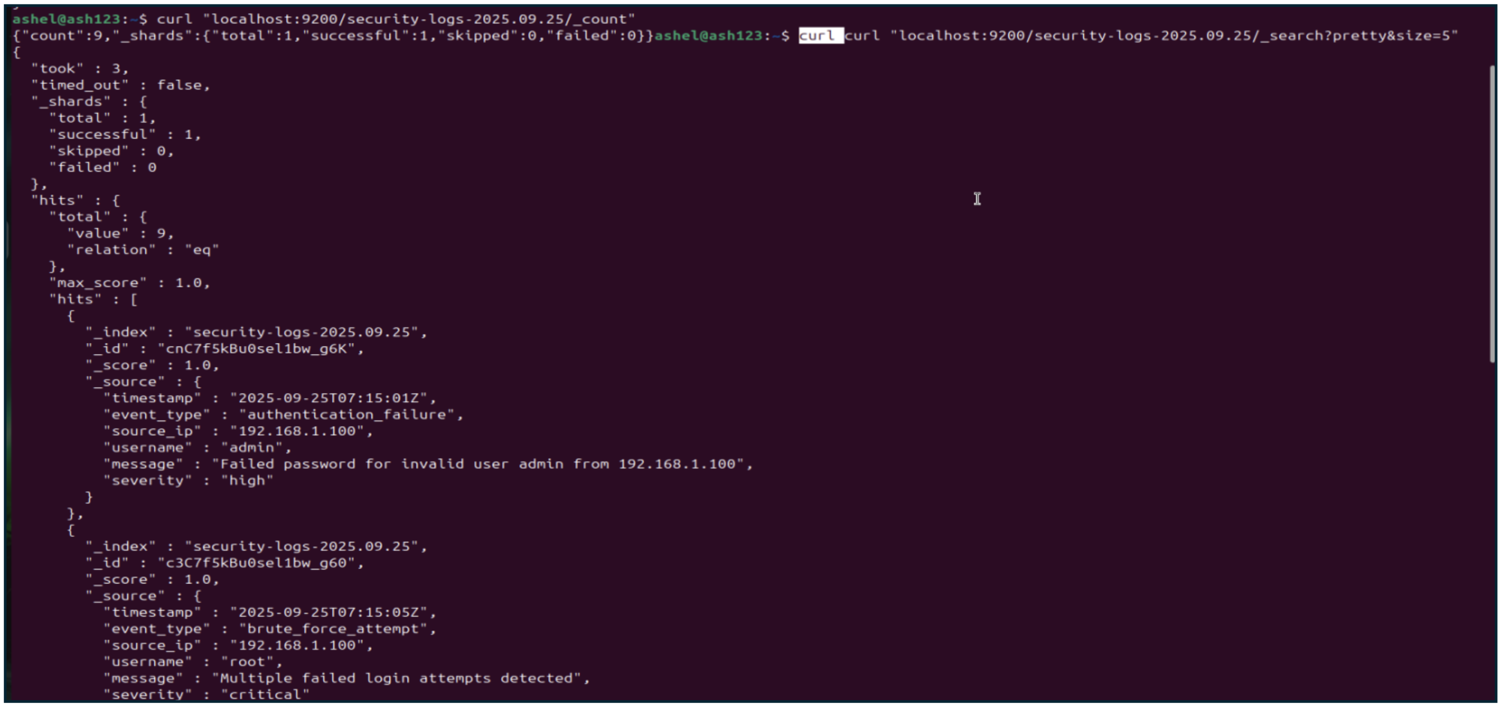
2. Screenshot of the Available fields showing event_type.keyword, severity.keyword, etc.



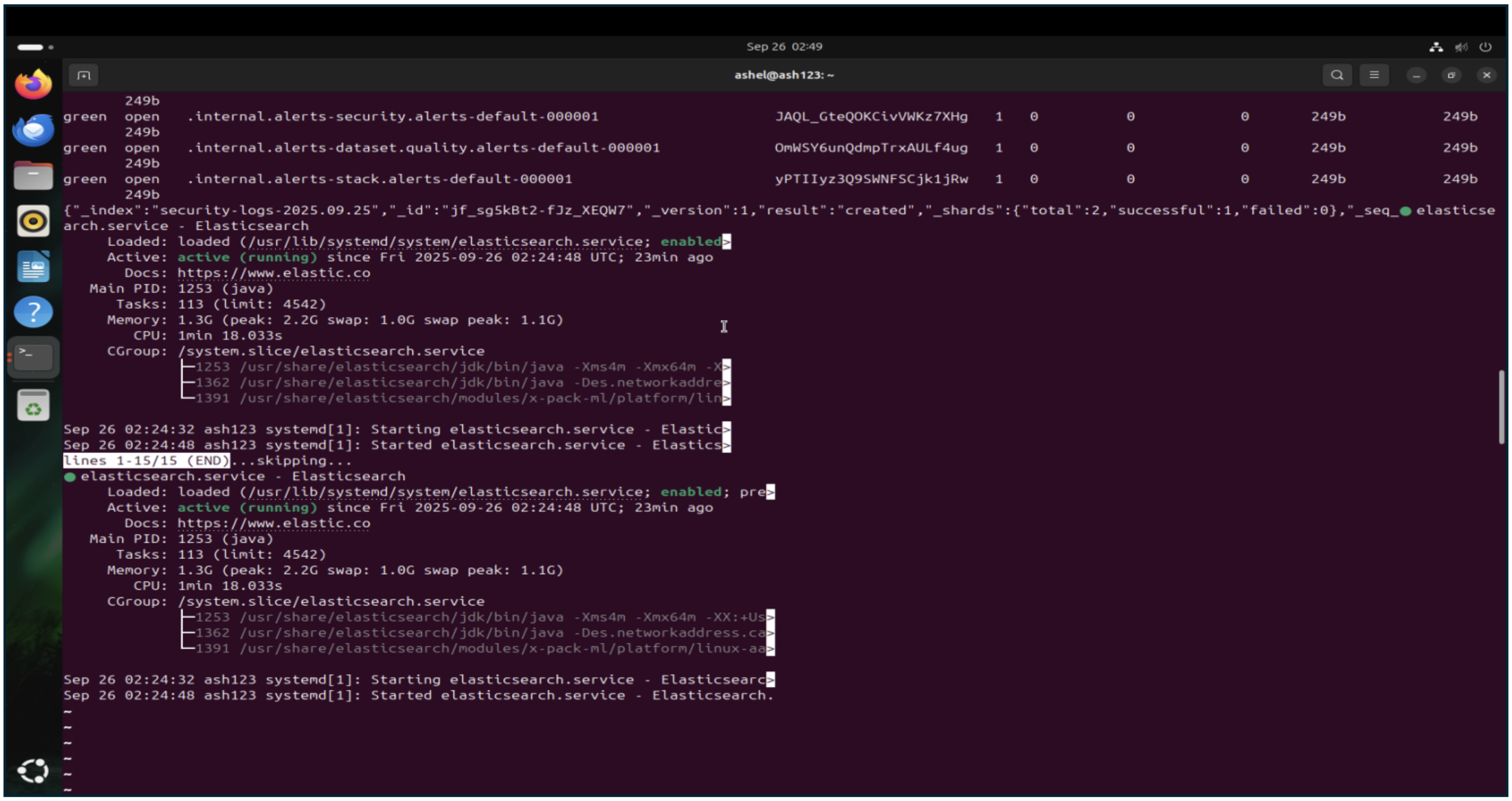
Available fields 10

- command.keyword
- event_type.keyword
- filename.keyword
- host.keyword
- message.keyword
- severity.keyword

3. Screenshot of terminal showing the curl commands working

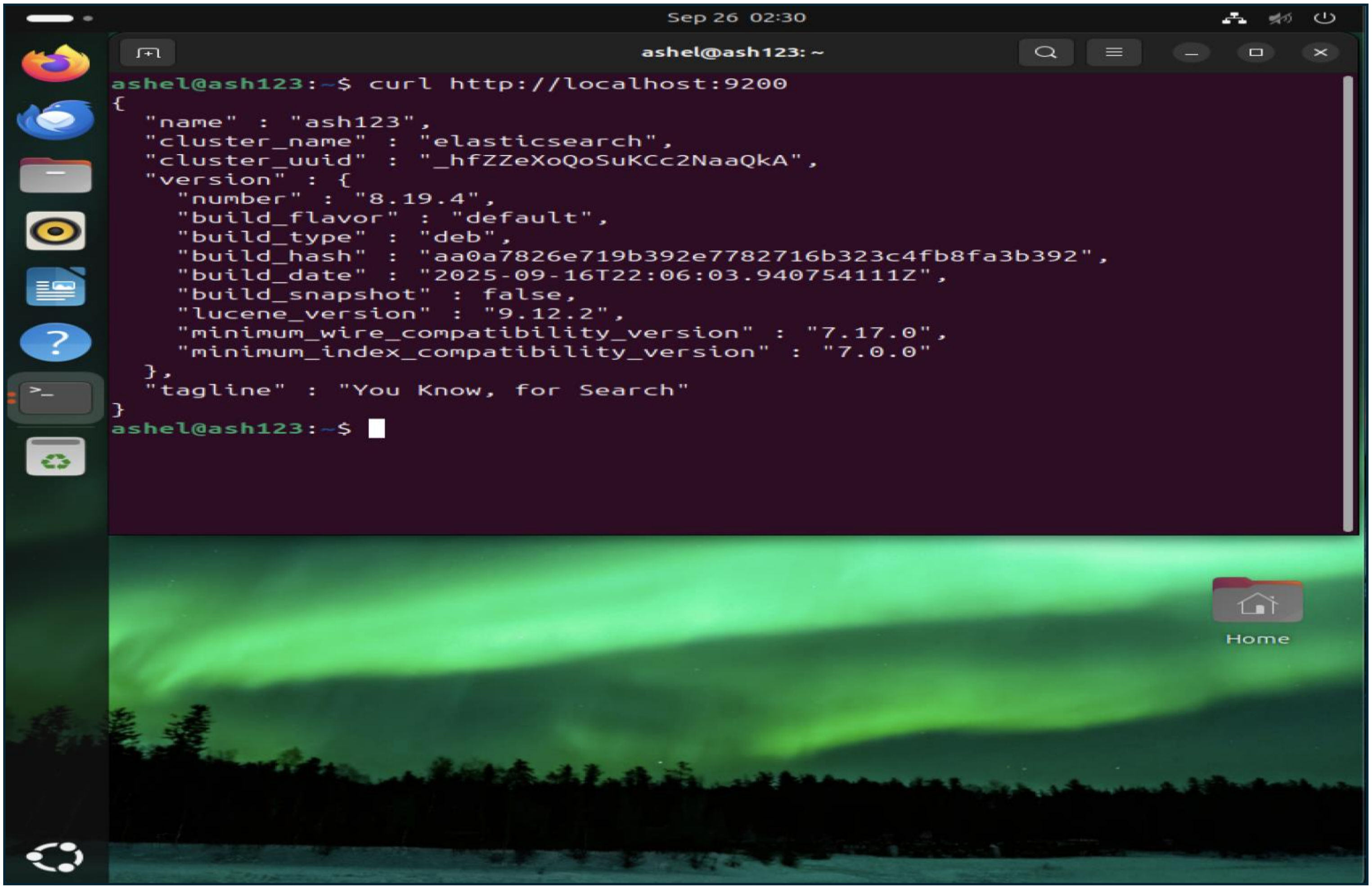


```
ashel@ash123:~$ curl "localhost:9200/security-logs-2025.09.25/_count"
{"count":9,"_shards":{"total":1,"successful":1,"skipped":0,"failed":0}}ashel@ash123:~$ curl curl "localhost:9200/security-logs-2025.09.25/_search?pretty&size=5"
{
  "took" : 3,
  "timed_out" : false,
  "_shards" : {
    "total" : 1,
    "successful" : 1,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 9,
      "relation" : "eq"
    },
    "max_score" : 1.0,
    "hits" : [
      {
        "_index" : "security-logs-2025.09.25",
        "_id" : "cnC7f5kBu0sel1bw_g6K",
        "_score" : 1.0,
        "_source" : {
          "timestamp" : "2025-09-25T07:15:01Z",
          "event_type" : "authentication_failure",
          "source_ip" : "192.168.1.100",
          "username" : "admin",
          "message" : "Failed password for invalid user admin from 192.168.1.100",
          "severity" : "high"
        }
      },
      {
        "_index" : "security-logs-2025.09.25",
        "_id" : "c3C7f5kBu0sel1bw_g60",
        "_score" : 1.0,
        "_source" : {
          "timestamp" : "2025-09-25T07:15:05Z",
          "event_type" : "brute_force_attempt",
          "source_ip" : "192.168.1.100",
          "username" : "root",
          "message" : "Multiple failed login attempts detected",
          "severity" : "critical"
```



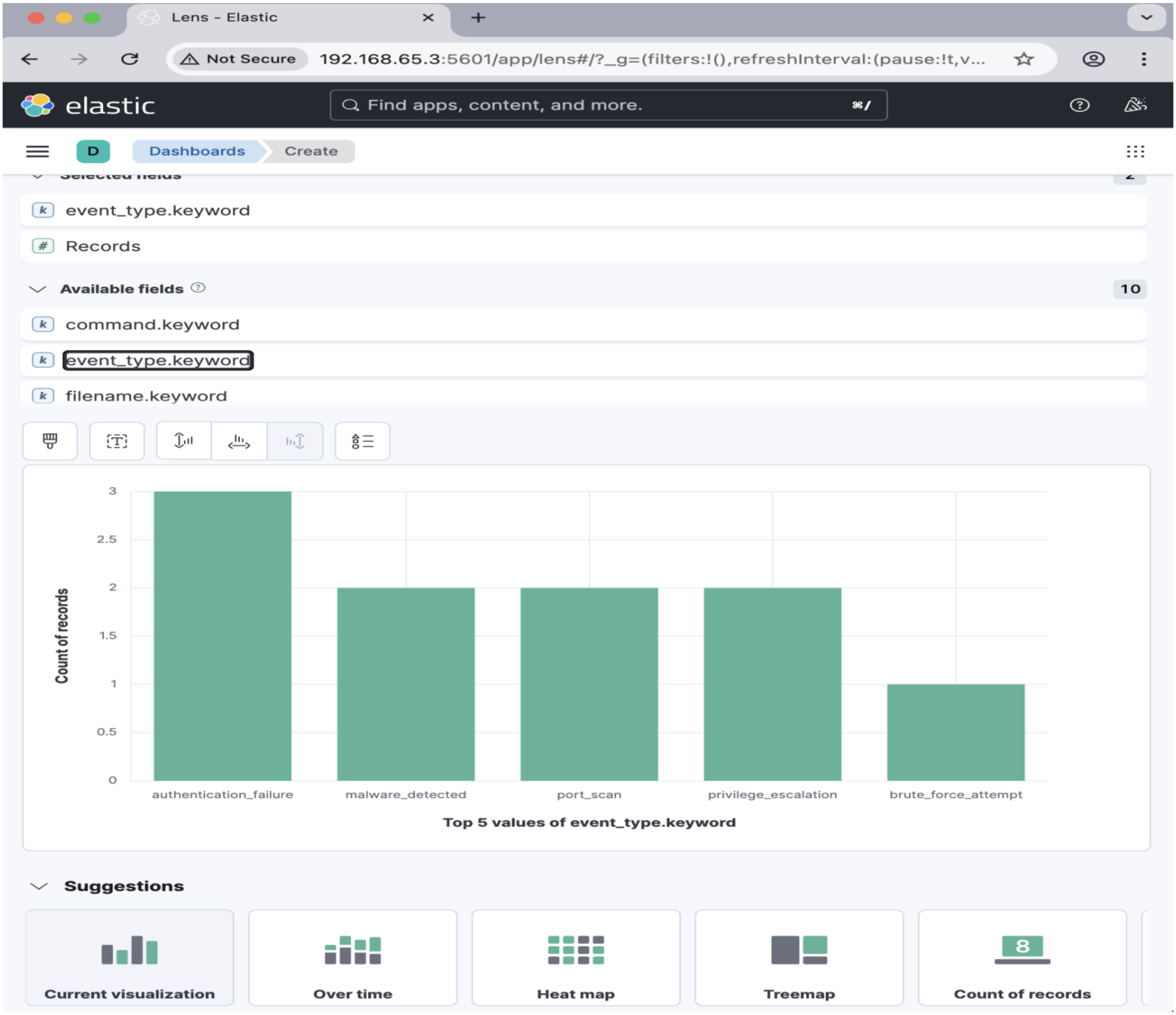
```
         249b
green  open   .internal.alerts-security.alerts-default-000001                    JAQL_GteQOKCivVWKz7XHg   1   0           0             0         249b             249b
         249b
green  open   .internal.alerts-dataset.quality.alerts-default-000001             OmWSY6unQdmpTrxAULf4ug   1   0           0             0         249b             249b
         249b
green  open   .internal.alerts-stack.alerts-default-000001                       yPTIIyz3Q9SWNFSCjk1jRw   1   0           0             0         249b             249b
         249b
{"_index":"security-logs-2025.09.25","_id":"jf_sg5kBt2-fJz_XEQW7","_version":1,"result":"created","_shards":{"total":2,"successful":1,"failed":0},"_seq_● elasticse
arch.service - Elasticsearch
     Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled>
     Active: active (running) since Fri 2025-09-26 02:24:48 UTC; 23min ago
       Docs: https://www.elastic.co
   Main PID: 1253 (java)
      Tasks: 113 (limit: 4542)
     Memory: 1.3G (peak: 2.2G swap: 1.0G swap peak: 1.1G)
        CPU: 1min 18.033s
     CGroup: /system.slice/elasticsearch.service
             ├─1253 /usr/share/elasticsearch/jdk/bin/java -Xms4m -Xmx64m -X>
             ├─1362 /usr/share/elasticsearch/jdk/bin/java -Des.networkaddre>
             └─1391 /usr/share/elasticsearch/modules/x-pack-ml/platform/lin>

Sep 26 02:24:32 ash123 systemd[1]: Starting elasticsearch.service - Elastic>
Sep 26 02:24:48 ash123 systemd[1]: Started elasticsearch.service - Elastics>
lines 1-15/15 (END)...skipping...
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; pre>
     Active: active (running) since Fri 2025-09-26 02:24:48 UTC; 23min ago
       Docs: https://www.elastic.co
   Main PID: 1253 (java)
      Tasks: 113 (limit: 4542)
     Memory: 1.3G (peak: 2.2G swap: 1.0G swap peak: 1.1G)
        CPU: 1min 18.033s
     CGroup: /system.slice/elasticsearch.service
             ├─1253 /usr/share/elasticsearch/jdk/bin/java -Xms4m -Xmx64m -XX:+Us>
             ├─1362 /usr/share/elasticsearch/jdk/bin/java -Des.networkaddress.ca>
             └─1391 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-aa>

Sep 26 02:24:32 ash123 systemd[1]: Starting elasticsearch.service - Elasticsearc>
Sep 26 02:24:48 ash123 systemd[1]: Started elasticsearch.service - Elasticsearch.
~
~
~
~
~
~
```

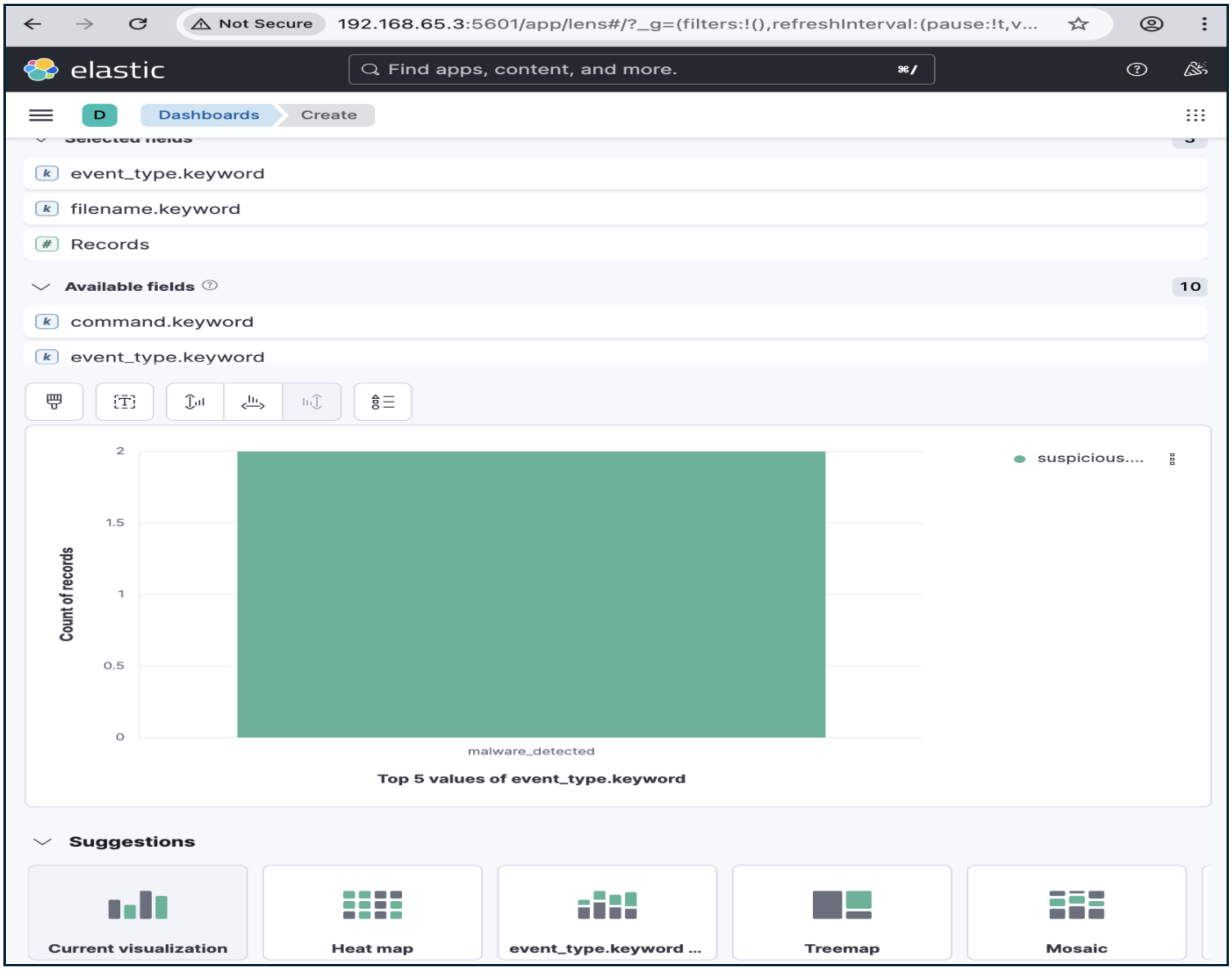
4. Screenshot of Elasticsearch status: `curl localhost:9200`



```
ashel@ash123:~$ curl http://localhost:9200
{
  "name" : "ash123",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "_hfZZeXoQoSuKCc2NaaQkA",
  "version" : {
    "number" : "8.19.4",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "aa0a7826e719b392e7782716b323c4fb8fa3b392",
    "build_date" : "2025-09-16T22:06:03.940754111Z",
    "build_snapshot" : false,
    "lucene_version" : "9.12.2",
    "minimum_wire_compatibility_version" : "7.17.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "You Know, for Search"
}
ashel@ash123:~$ 
```

5. Screenshot of analysis




Not Secure
192.168.65.3:5601/app/lens#/?_g=(filters:!(),refreshInterval:(pause:!t,v...
elastic
Find apps, content, and more.
⌘/
D
Dashboards
Create
Selected fields
3

event_type.keyword

filename.keyword

Records

command.keyword

event_type.keyword