Anomaly Detection with Splunk

What is Splunk?

SIEM, such as an Splunk, is an important part of a security analyst's toolbox because it provides a platform for storing, analyzing, and reporting on data from different sources. The Splunk's querying language, called Search Processing Language (SPL), includes the use of pipes and wildcards. In addition, the effective search helps us efficiently identify patterns, trends, and anomalies within data.

Question: Identify anomalies in http logs.

Steps

- Ingest data into Splunk
- Index and parse
- **Query** the logs for high volumes of error responses (>=400):

```
index=_* OR index=* sourcetype=http_log | stats count by response | where response >= 400
```

Results (top 5 due to space):

response	count
404	137764
400	72
500	2
401	1
403	1