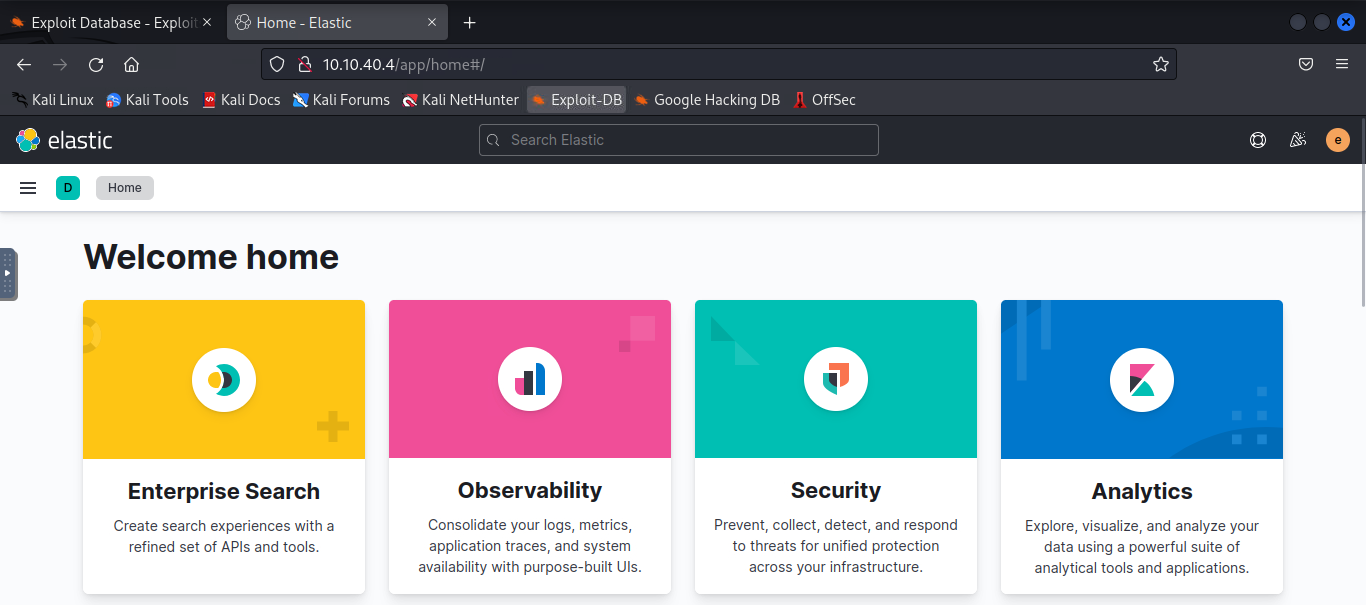
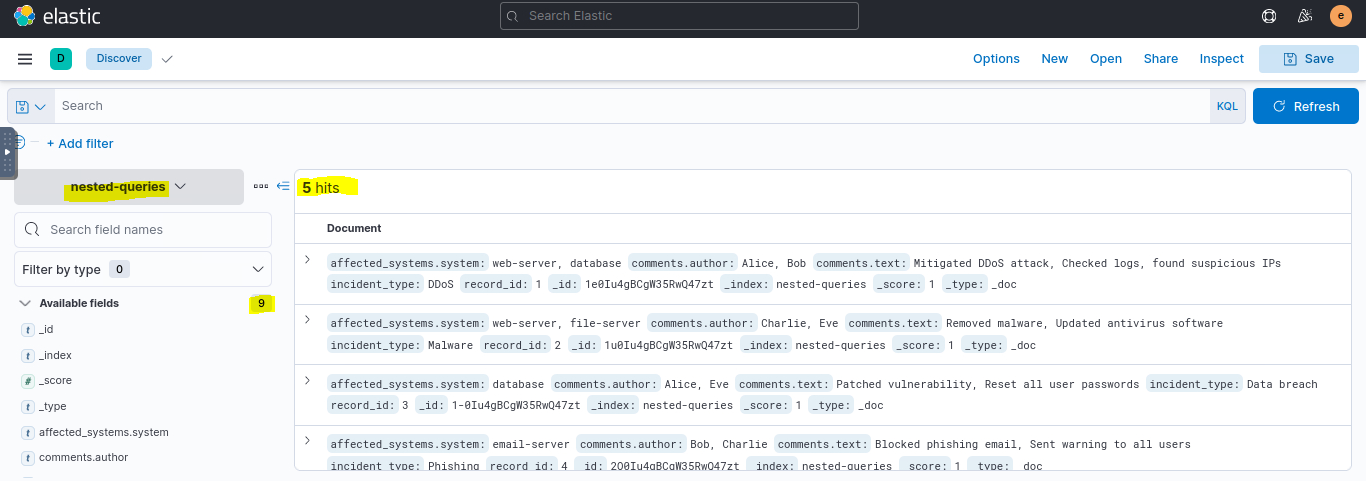
Advanced Elk

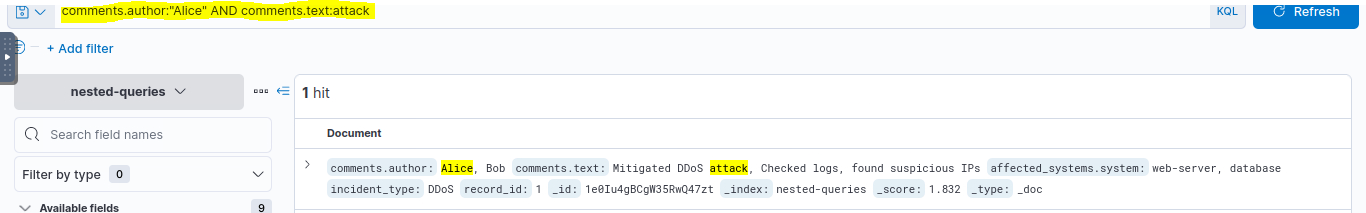
Elastic



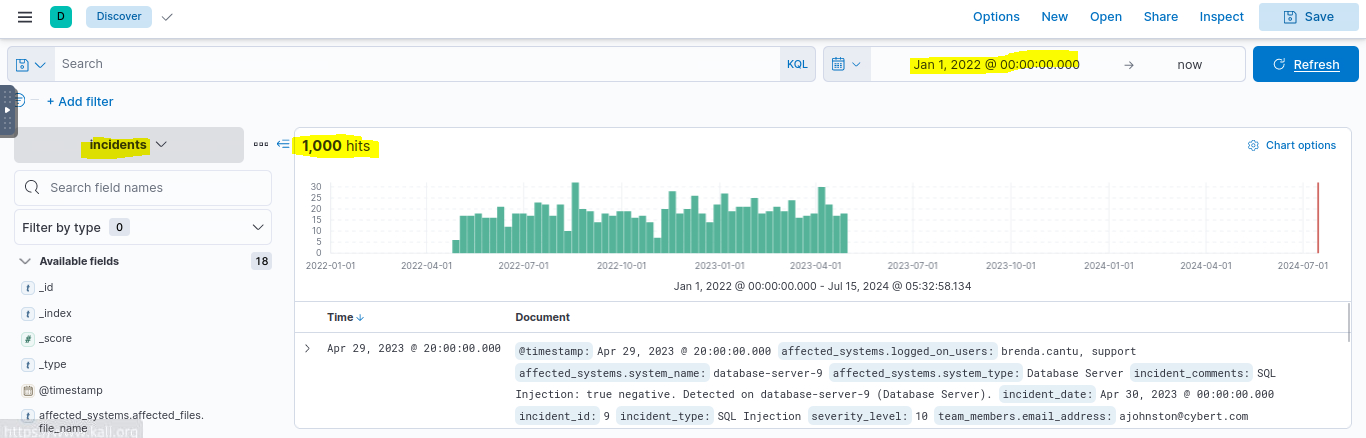
Discover



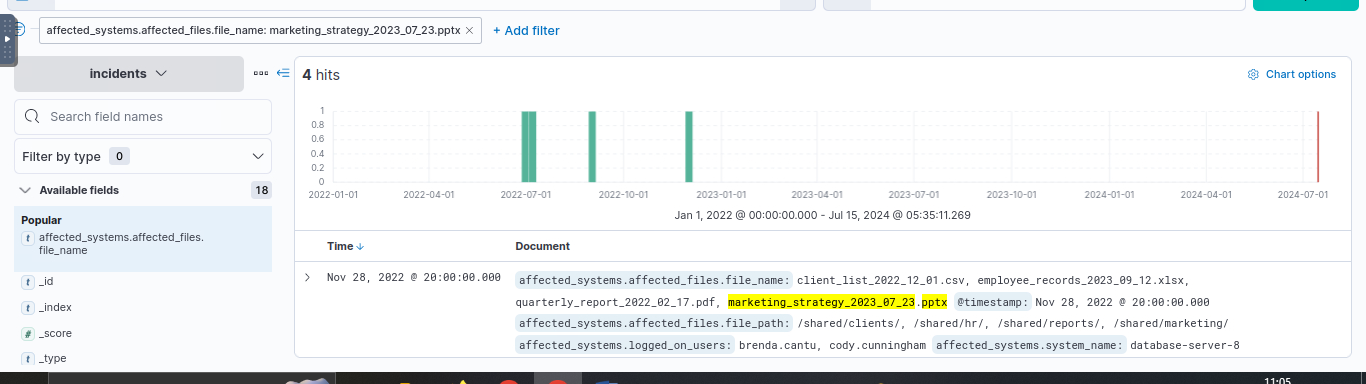
Query



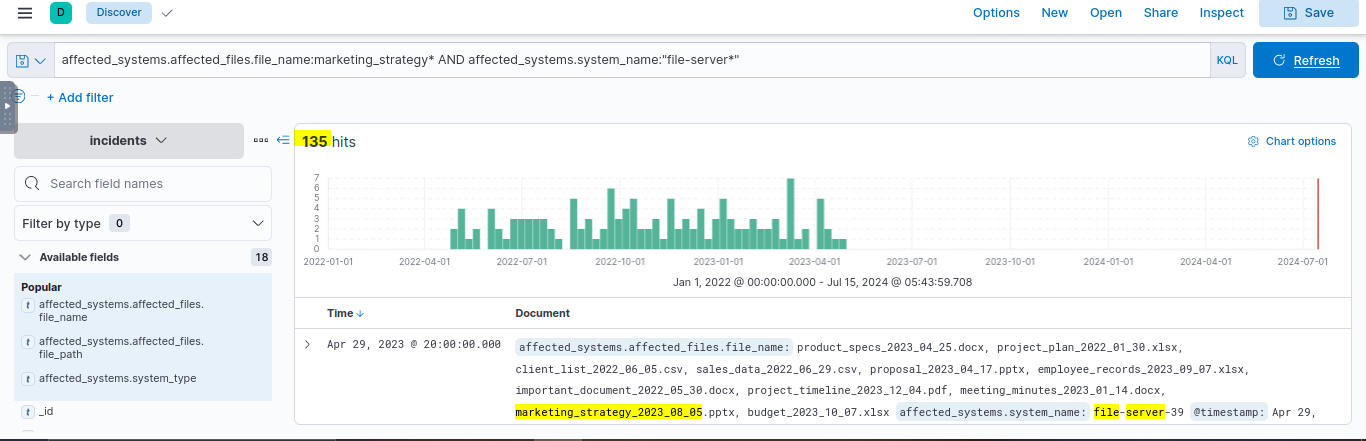
Incidents from jan 1 2022 till now. 1000 Hits



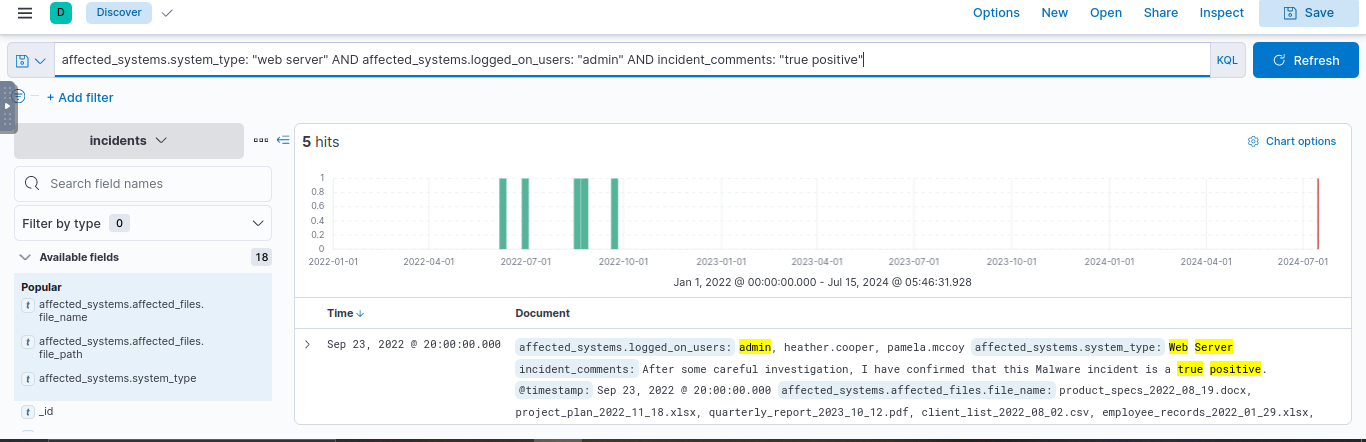
Affected file name hits



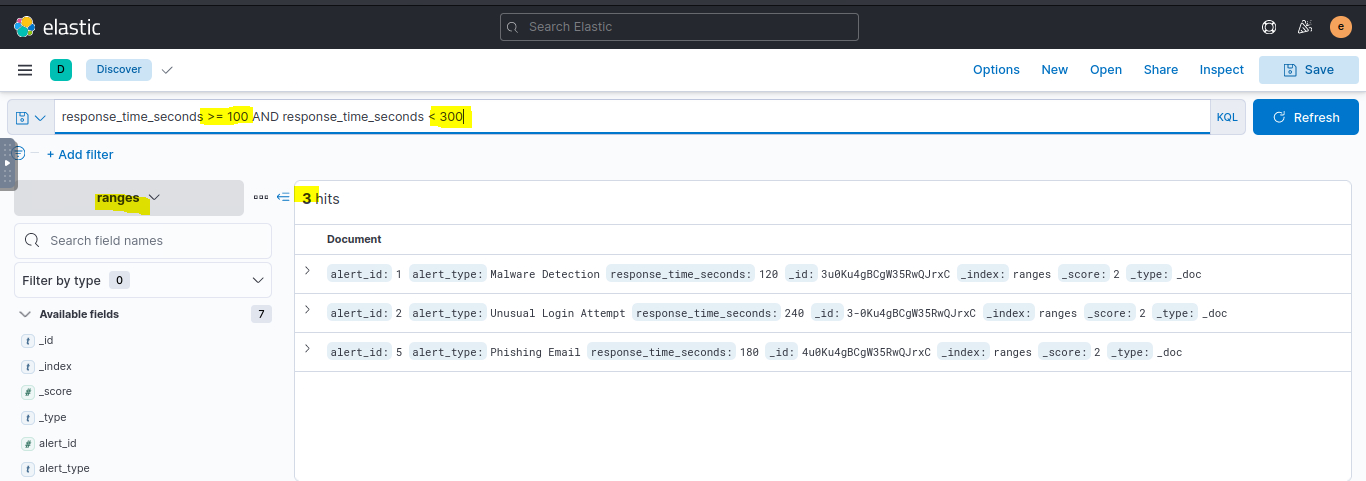
File Server



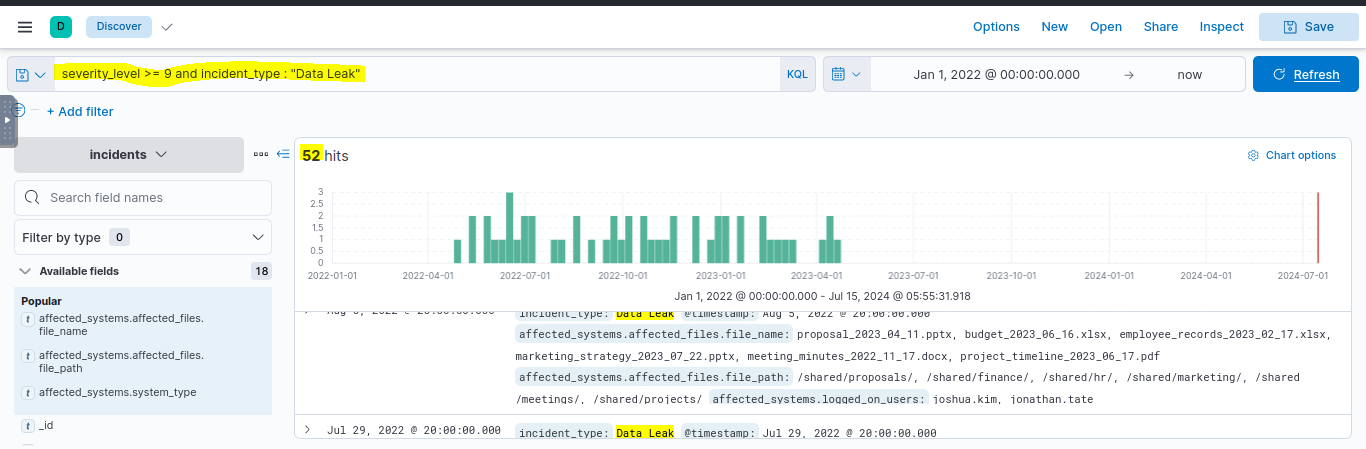
True positive admin login



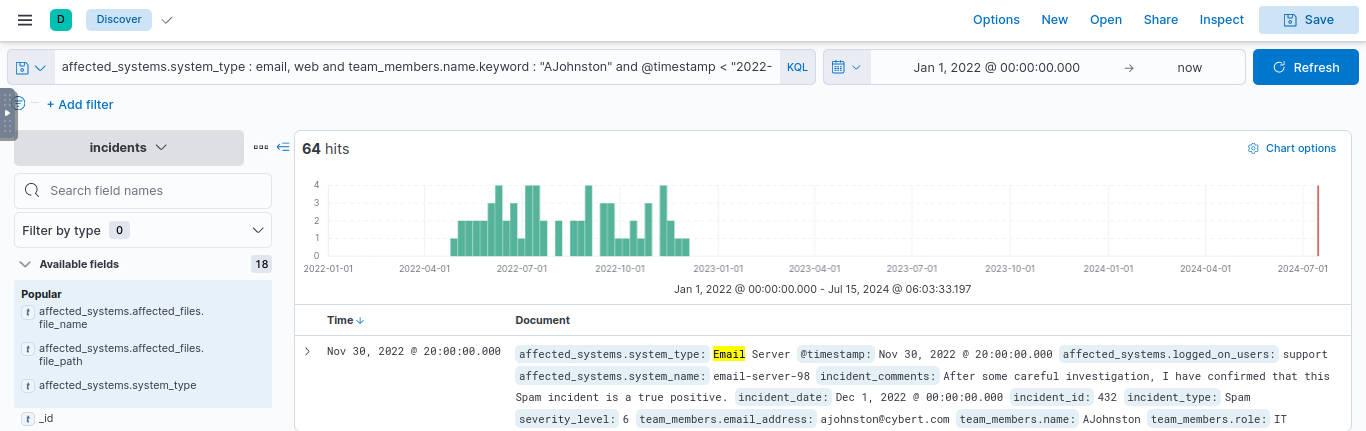
**Ranges**



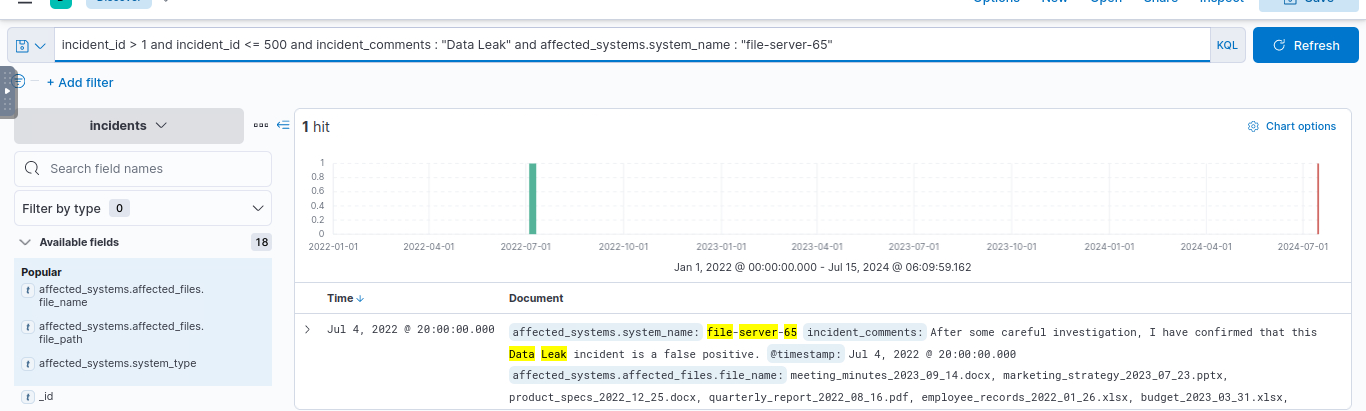
Data leak with severity



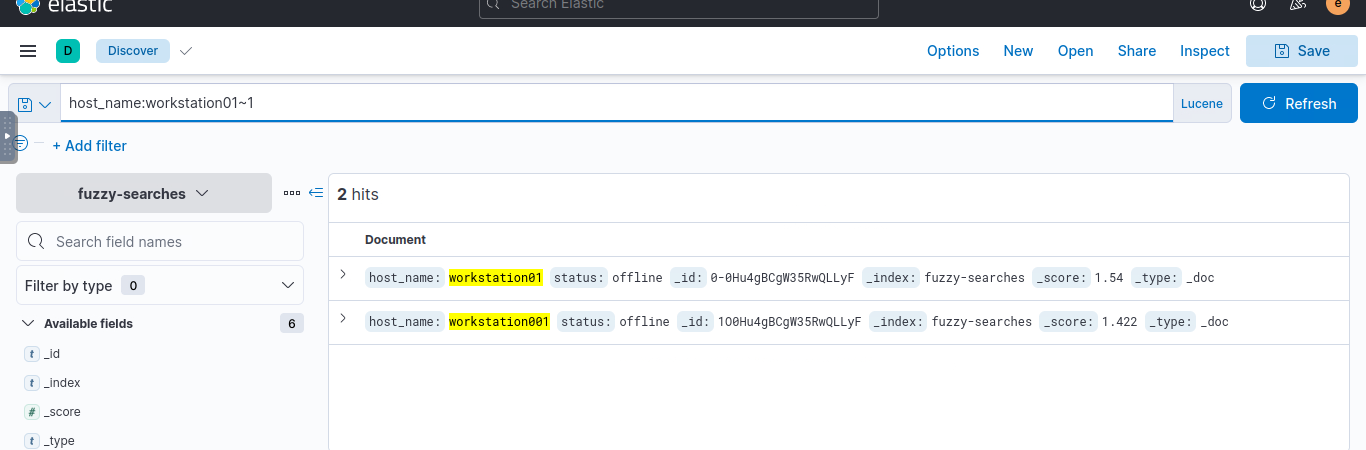
Time stamp before December 1



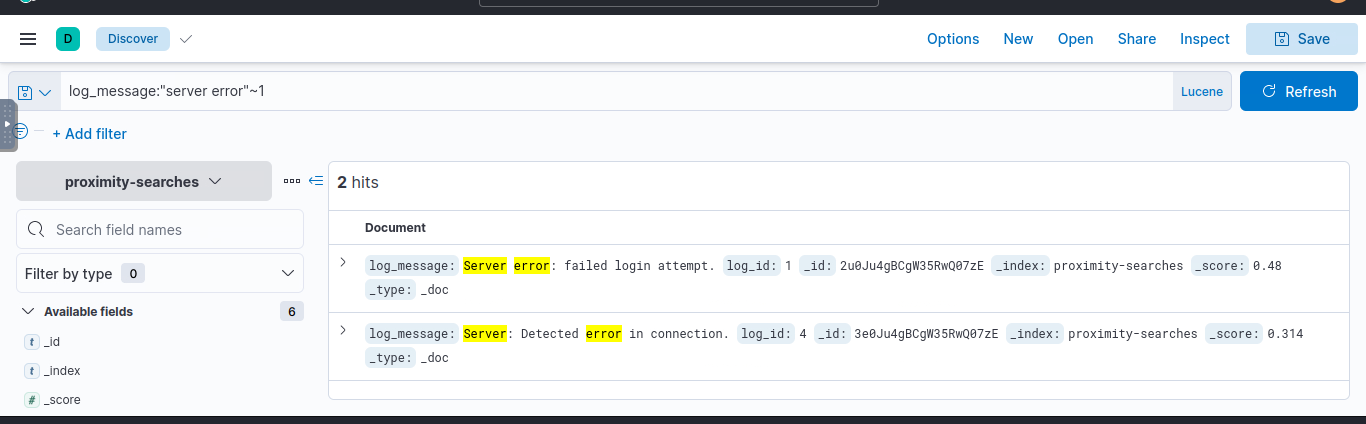
incident\_id > 1 and incident\_id <= 500 and incident\_comments : "Data Leak" and affected\_systems.system\_name : "file-server-65"



Lucene – fuzzy search



Proximity searches



Regular expressions: all event types

