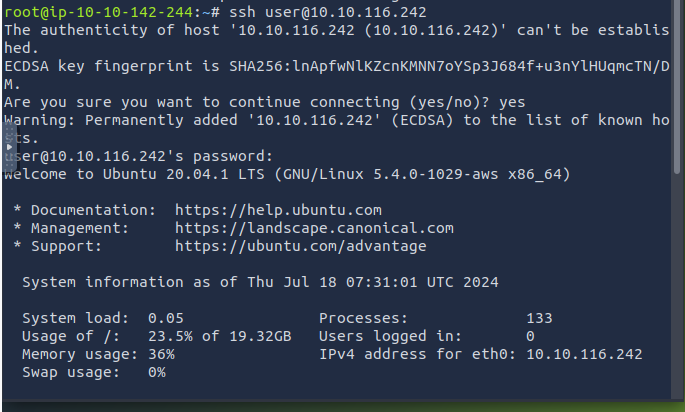
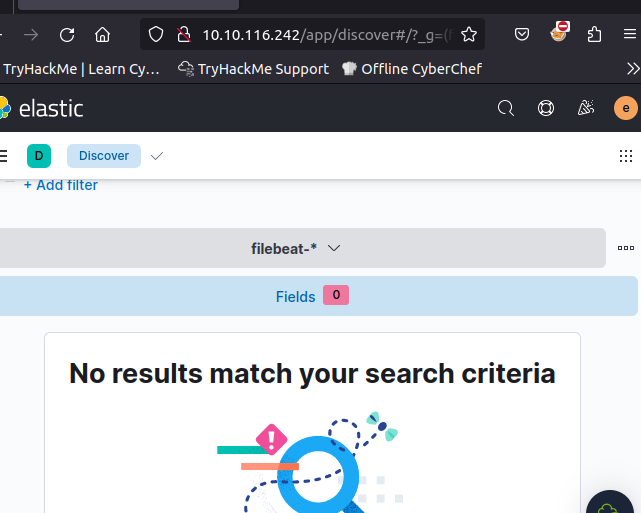
Threat intelligence for soc

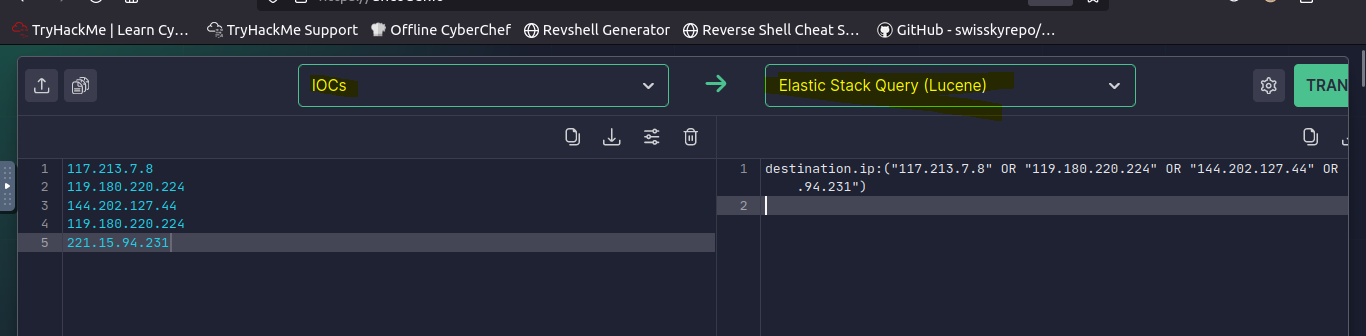
SSh access to the machine



Kibana instance through the ssh logged in machine



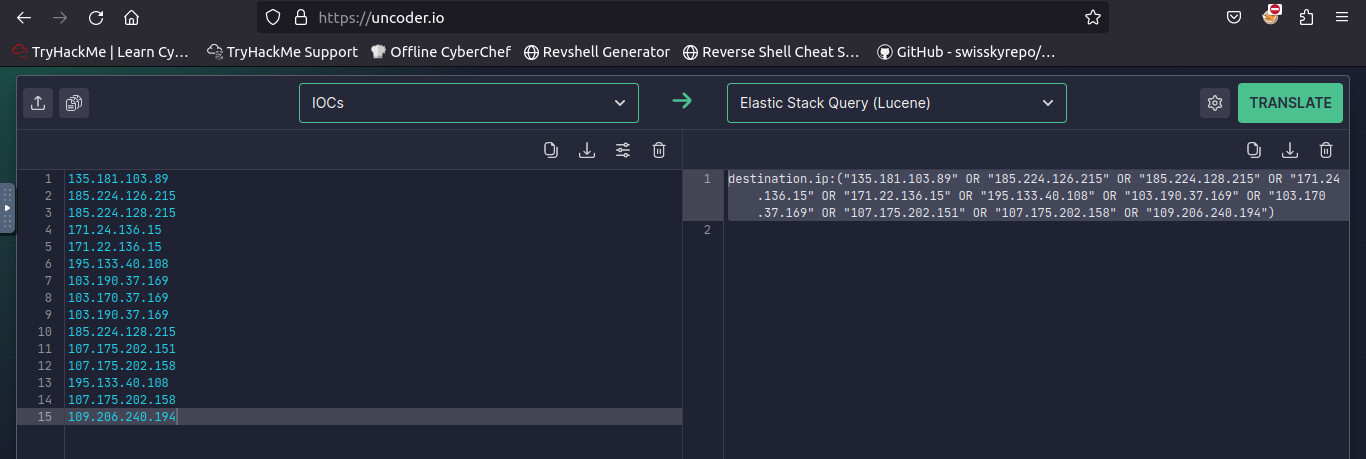
Uncoder List of iocs translated to elastic stack query



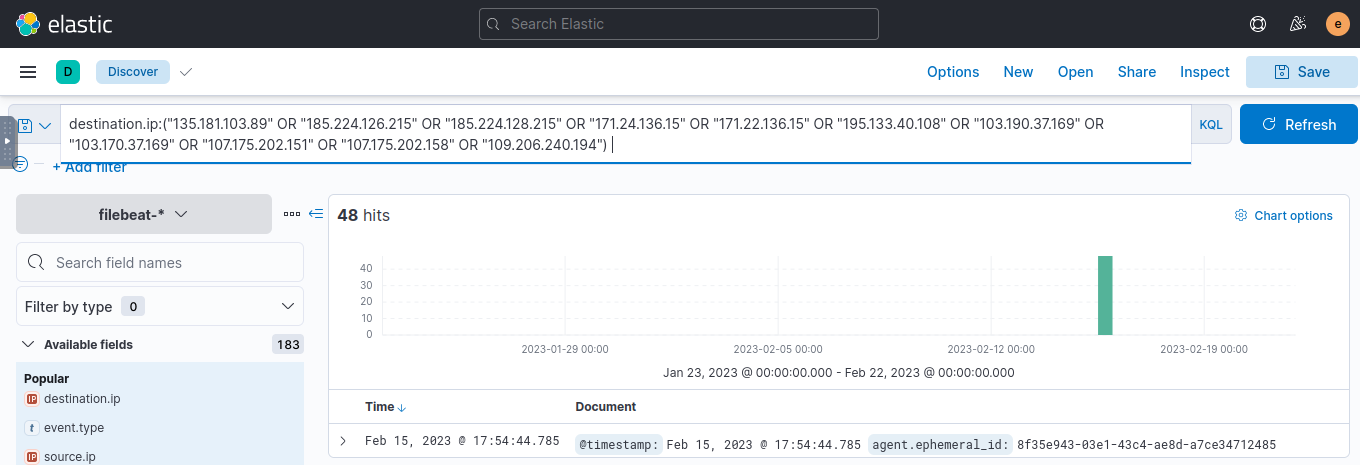
The number of hits in the timeframe



Different ioc list of 15 entries – 11 ip addresses

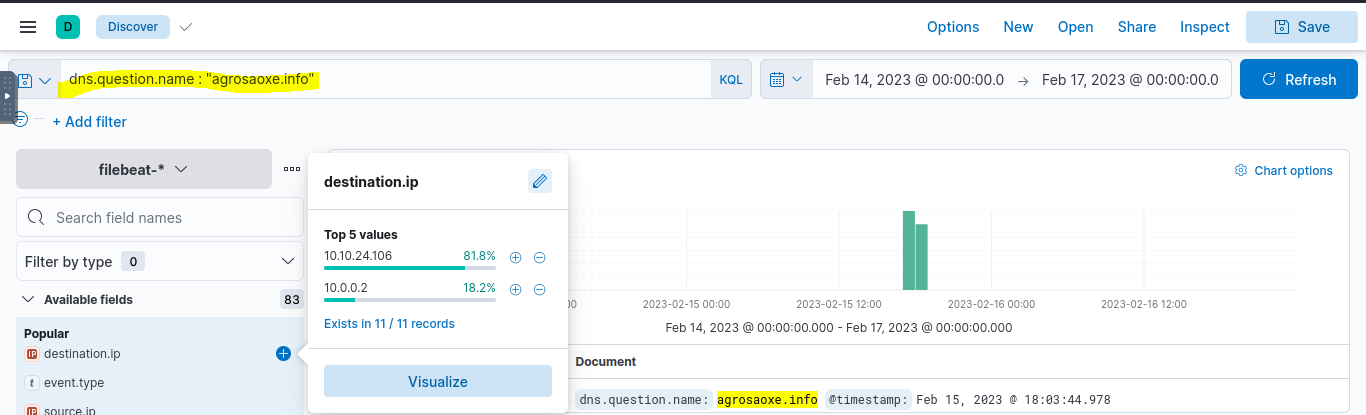


Based on the ioc list : the number of hits

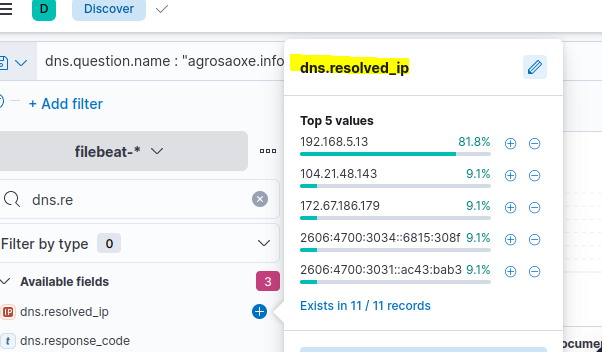


DNS PREVENTION

Dns question for the particular domain name



Dns resolved ip

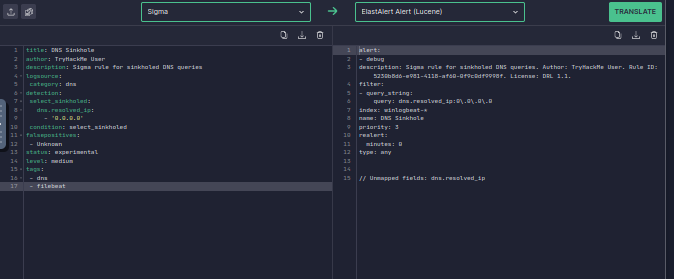


192.168.5.13 – the sinkhole ip

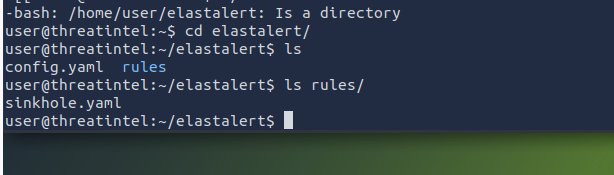
Next two are resolved ip

Threat detection

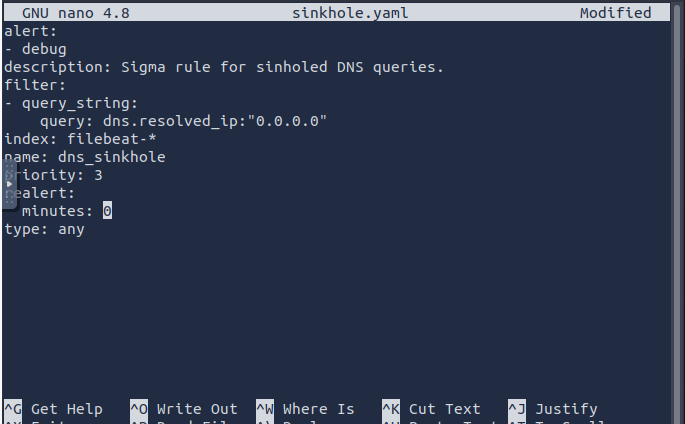
Sigma rule to elastalert



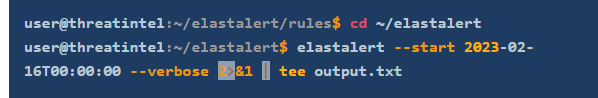
Ssh to the machine and the files



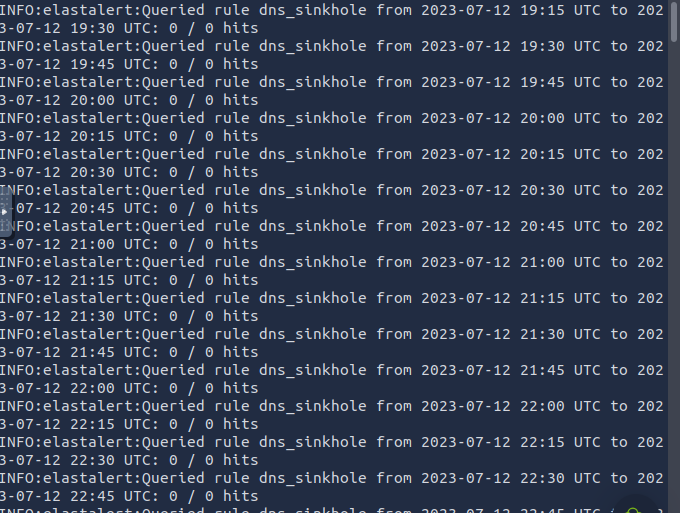
The translated elasalert to sinkhole.yaml



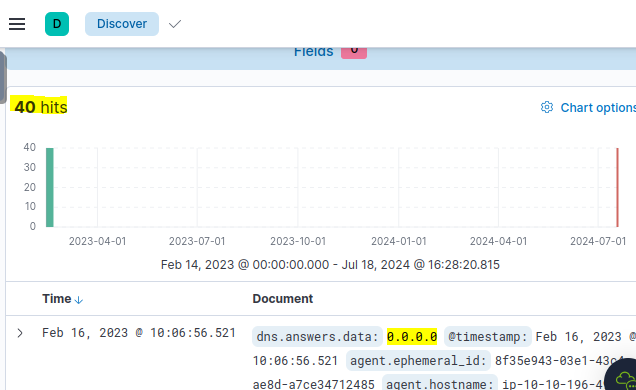
Running the command to start



Running



Alerts created by the rule



Unique sinkholes

