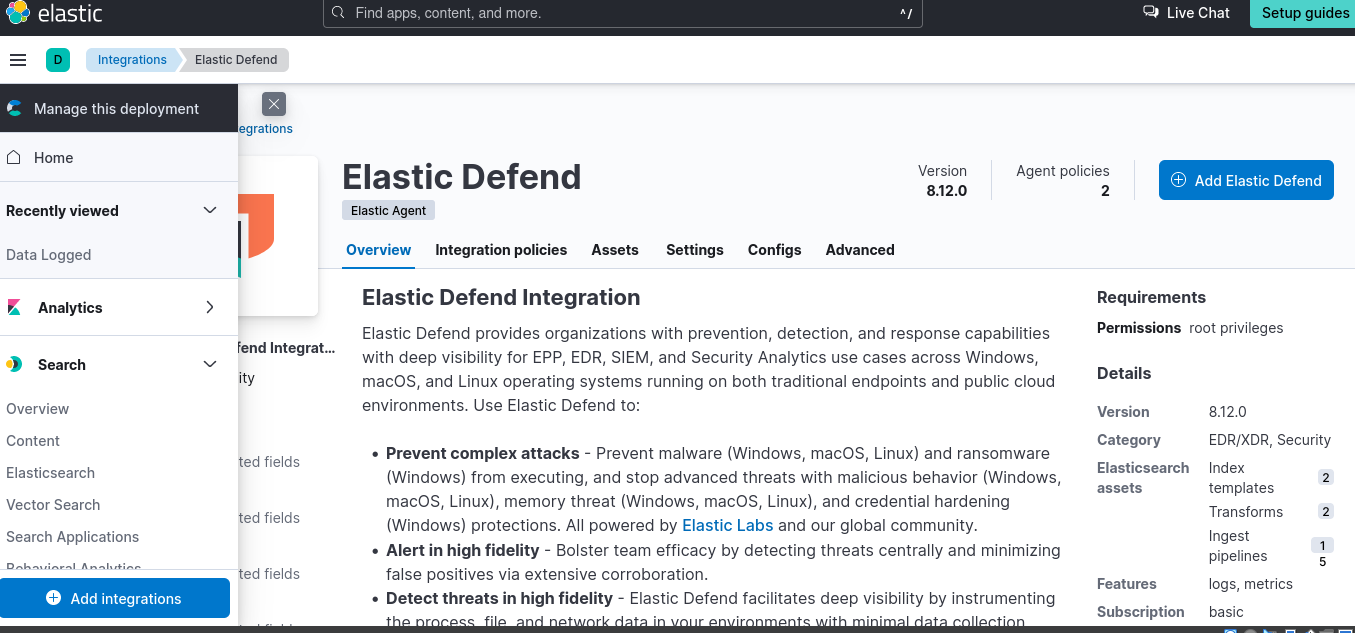
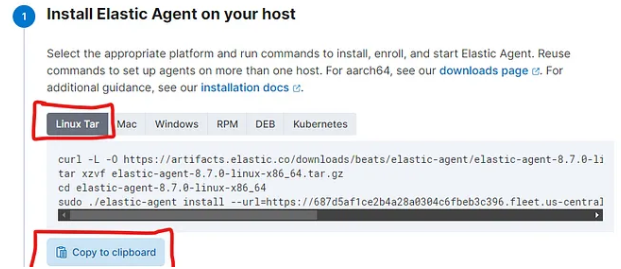
Elastic SIEM Lab

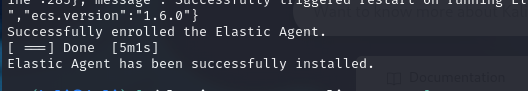
In this Home Lab I set up for Elastic Stack Security Information Event Management using the elastic web portal and Kali VM. Within this lab I was able to generate security events on Kali VM, set up an agent that forwards data to the SIEM as well as query and analyze logs in the SIEM. Very beneficial lab that continues to provide me with hands-on experience in working with different tools to help sharpen my analyst skills.

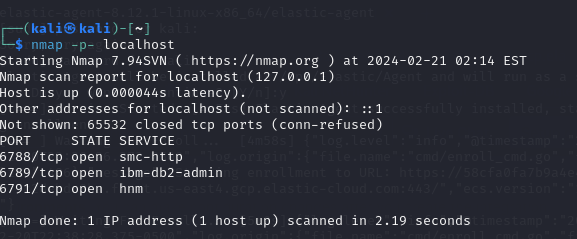
1. Set up agent “Elastic Defend” that will collect logs from my Kali VM and push data to Elastic SIEM

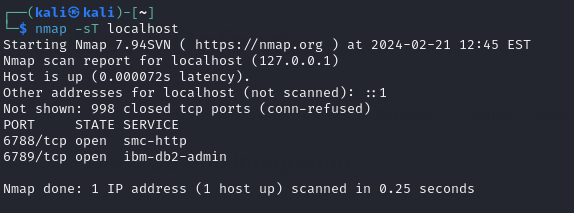


Next was to copy command to enter into LInux terminal

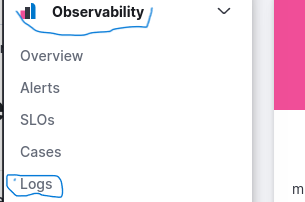
Entered and successfully installed Elastic agent into Linux VM



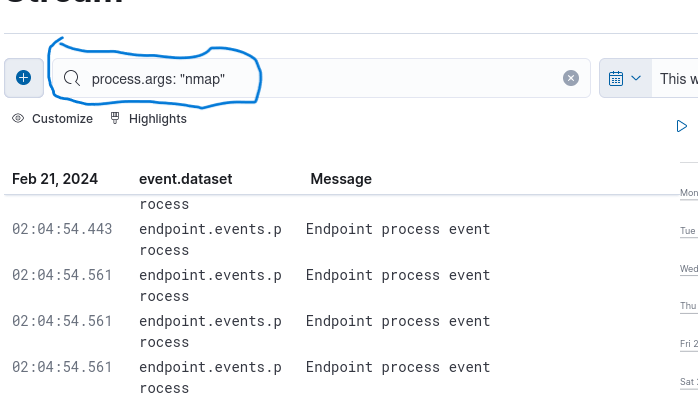
After installing Elastic agent next I was able to able generate Security events on Kali VM, this was done using Network analyzer Nmap so I ran the following commands to generate security events: 



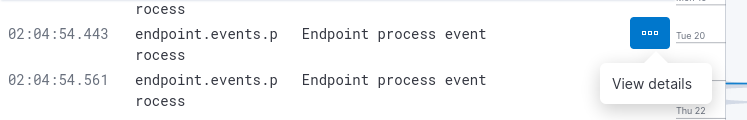
Now I have forwarded data from kali VM to the SIEM im able to query and analyze logs within the SIEM

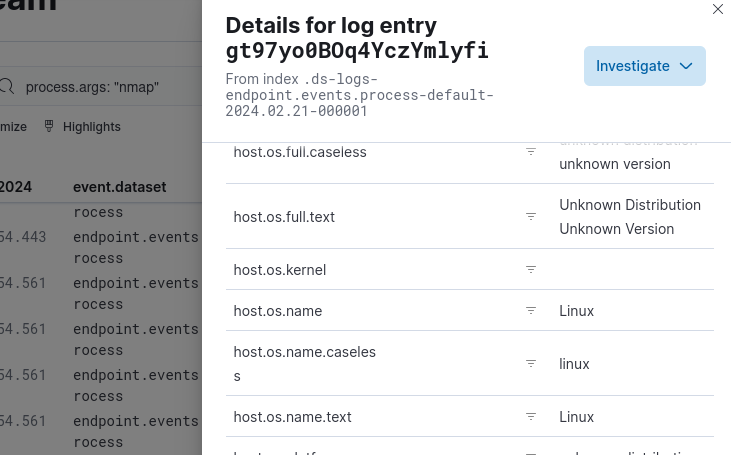


Next was to enter search query to filter the logs that was generated with our scans

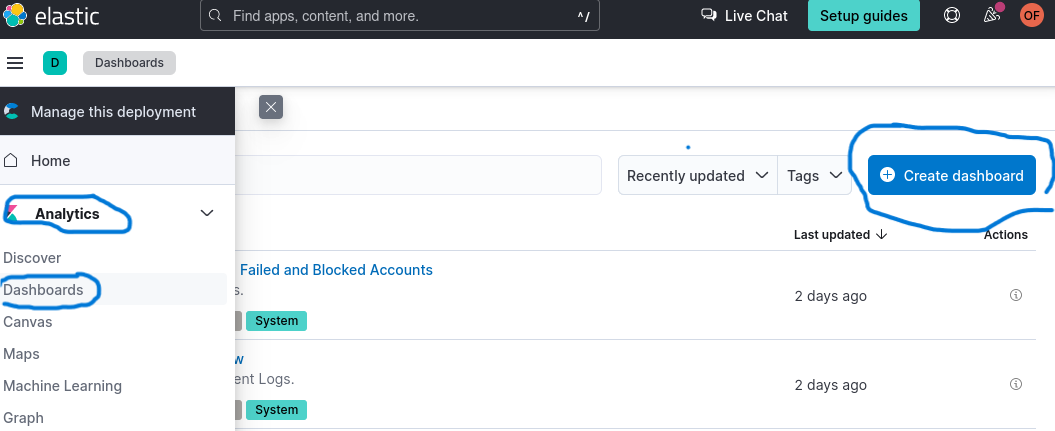


With Security events on display I was able to gather details on Security events giving me more details on the events.

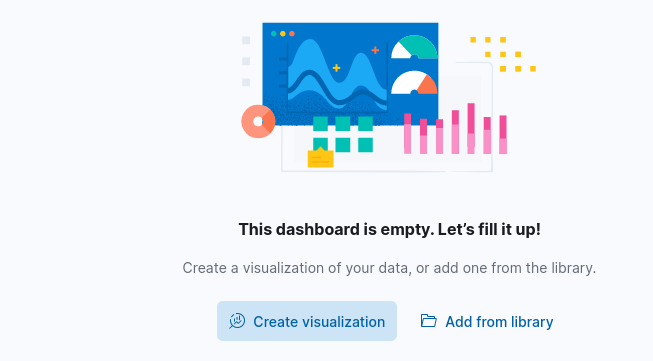


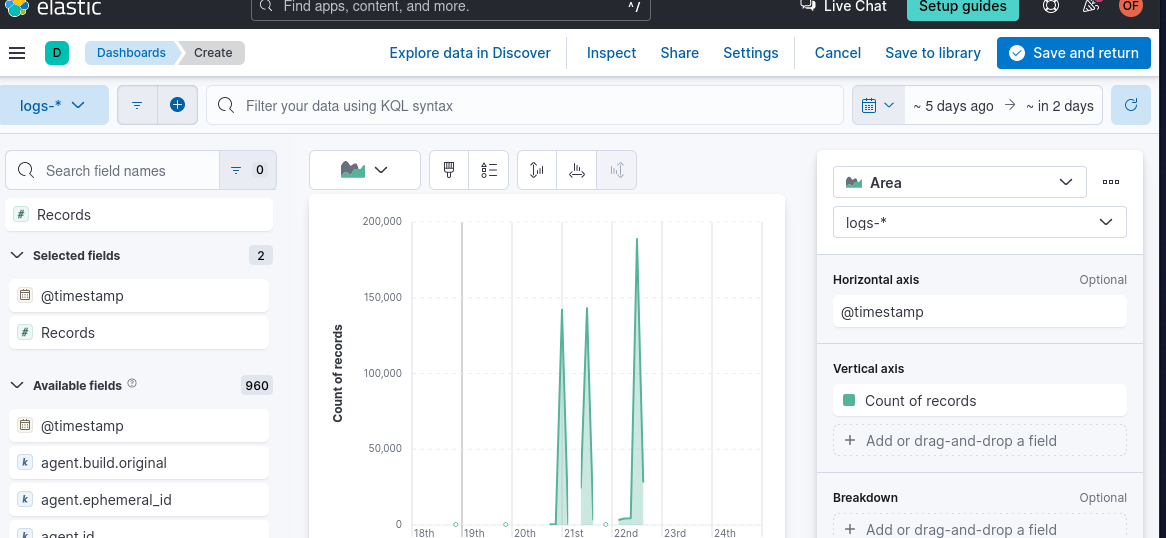


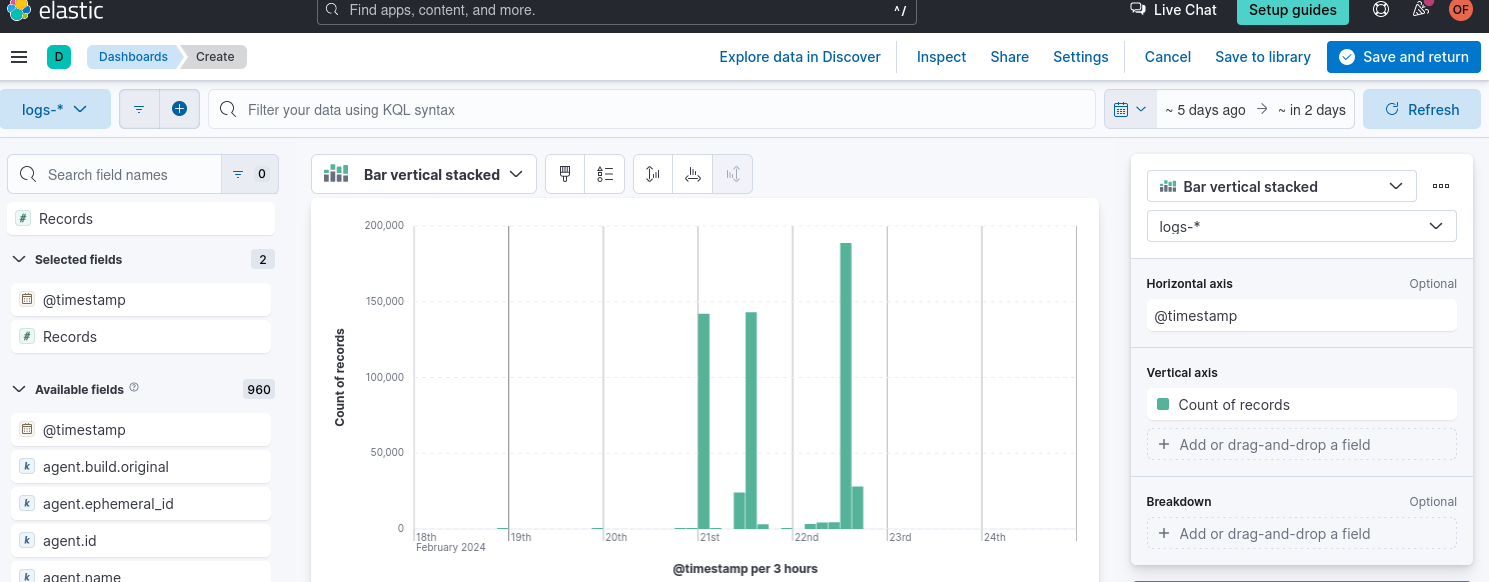
Next tasks was to create dashboards and visualizations within the SIEM to further analyze logs and identify if they may be patterns to be aware of data that's just not of the norm.



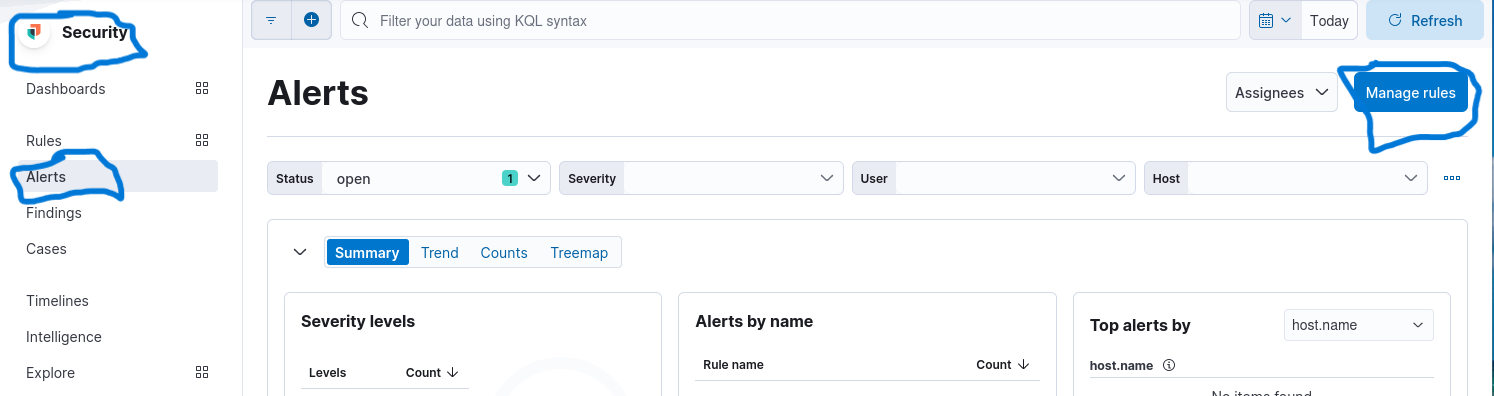
Next I added Visualization to the dashboard to help see a visual of the data of events

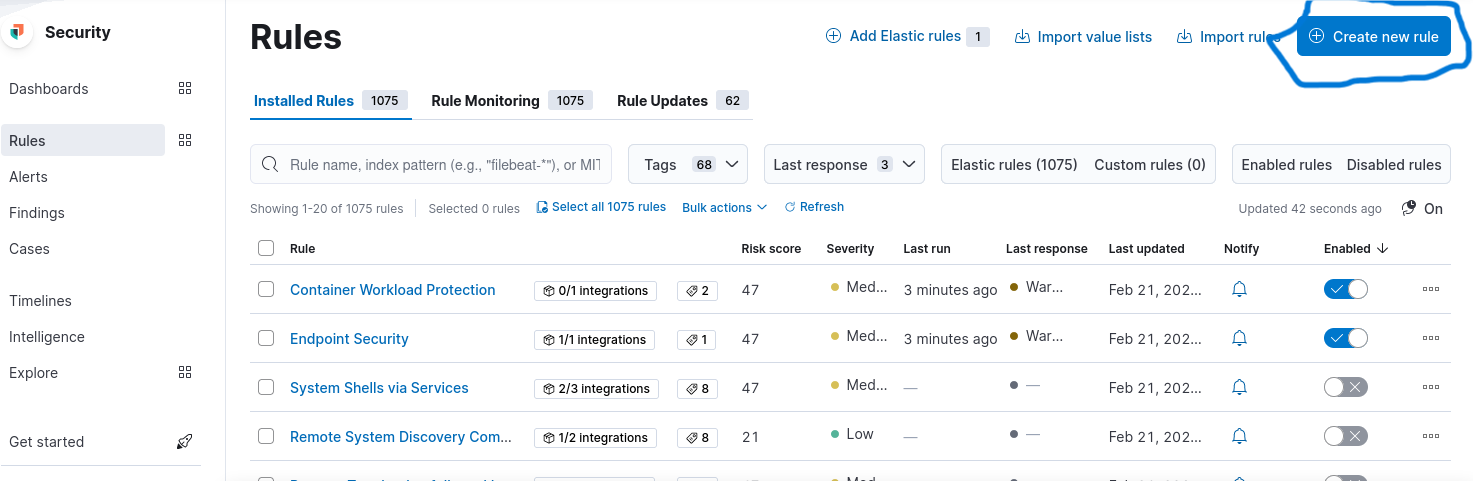




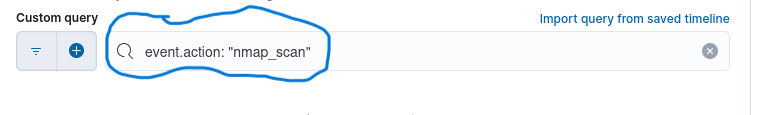
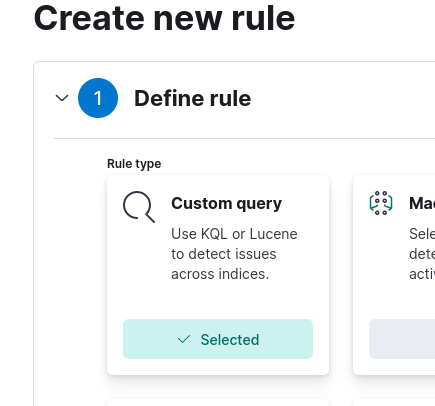


The next task was to create an alert which can be a critical feature used to detect security incidents and being able to respond in a timely manner, and can be configured to trigger specific actions when conditions of alert are met.





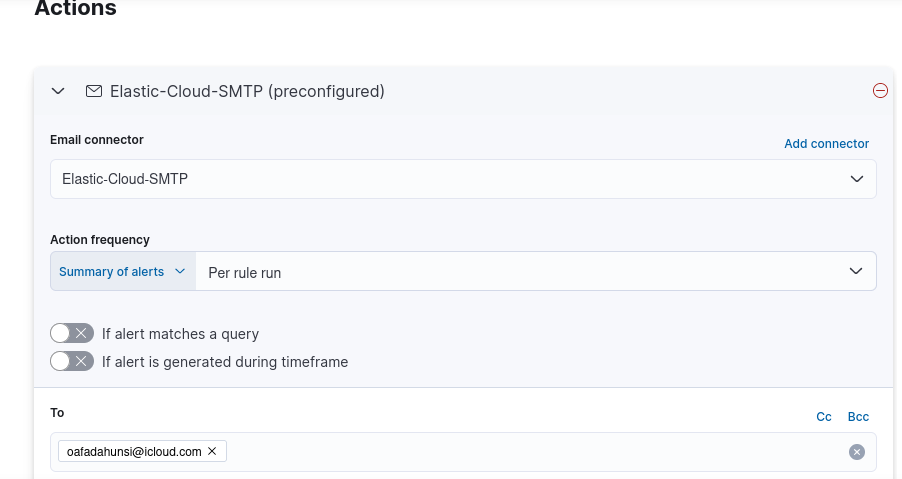
Next step was create new rule within the custom query selection to detect all Nmap scan events



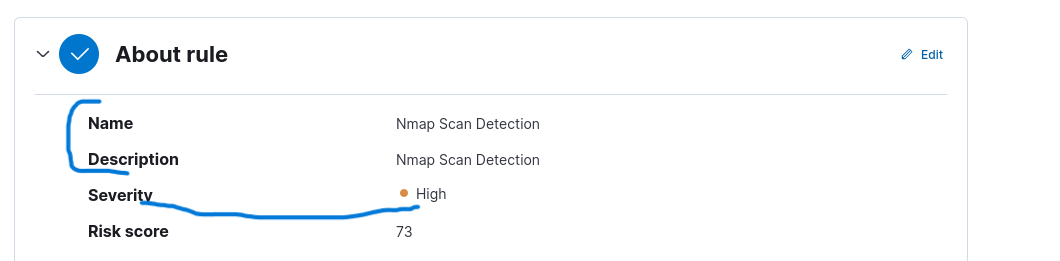
Next leading up to final tasks we defined the rule



The last few steps before finalizing the rule was to give my rule a name and description and notify me by email once the alert is triggered.



Before the final task was to create name and description of the rule along with the severity of importance which will help prioritize what needs to be done



Final task is to click create and enable the rule button to finally create the rule.



Once a rule is created it will monitor logs for Nmap scan events if an alert is triggered the selected action that is chosen will be implemented.

In this Lab, I was able to set up a home lab using Elastic SIEM and a Kali VM. The data was forwarded from the Kali VM to the SIEM using the Elastic agent, generated security events on the Kali VM using Nmap, queried and analyzed the logs in the SIEM using the Elastic web interface. Also I created a dashboard to visualize security events and then create an alert to detect security events.

This home lab provided me with a valuable environment for learning and practicing the skills necessary for effective security monitoring and incident response using Elastic SIEM.