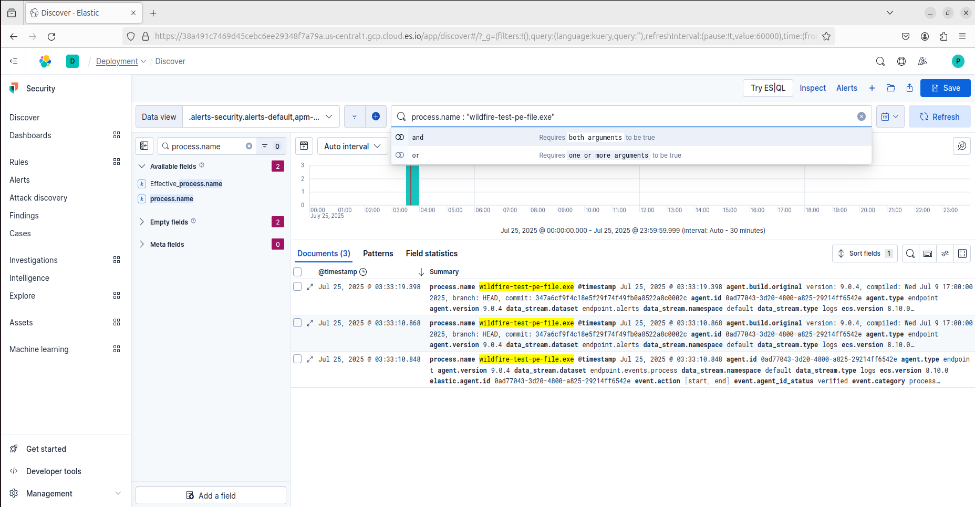
Sample Test on getting Alerts in Elastic:

I have downloaded a sample malicious test file with name “wildfire-test-pe-file”.

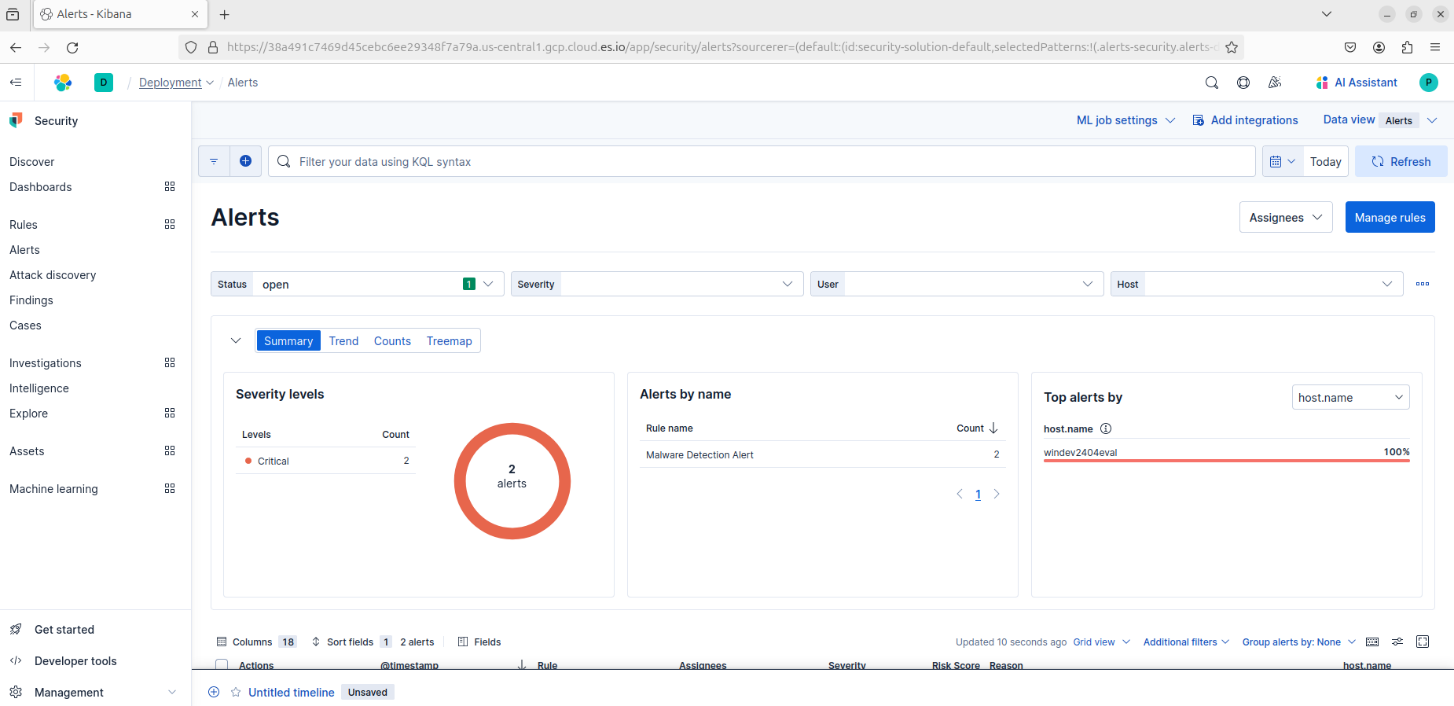
After downloading the file in windows VM, we can see that the logs from event.dataset: zeek.http and the alerts can be found in alerts section with high risk and needs immediate attention.

Screenshots below:

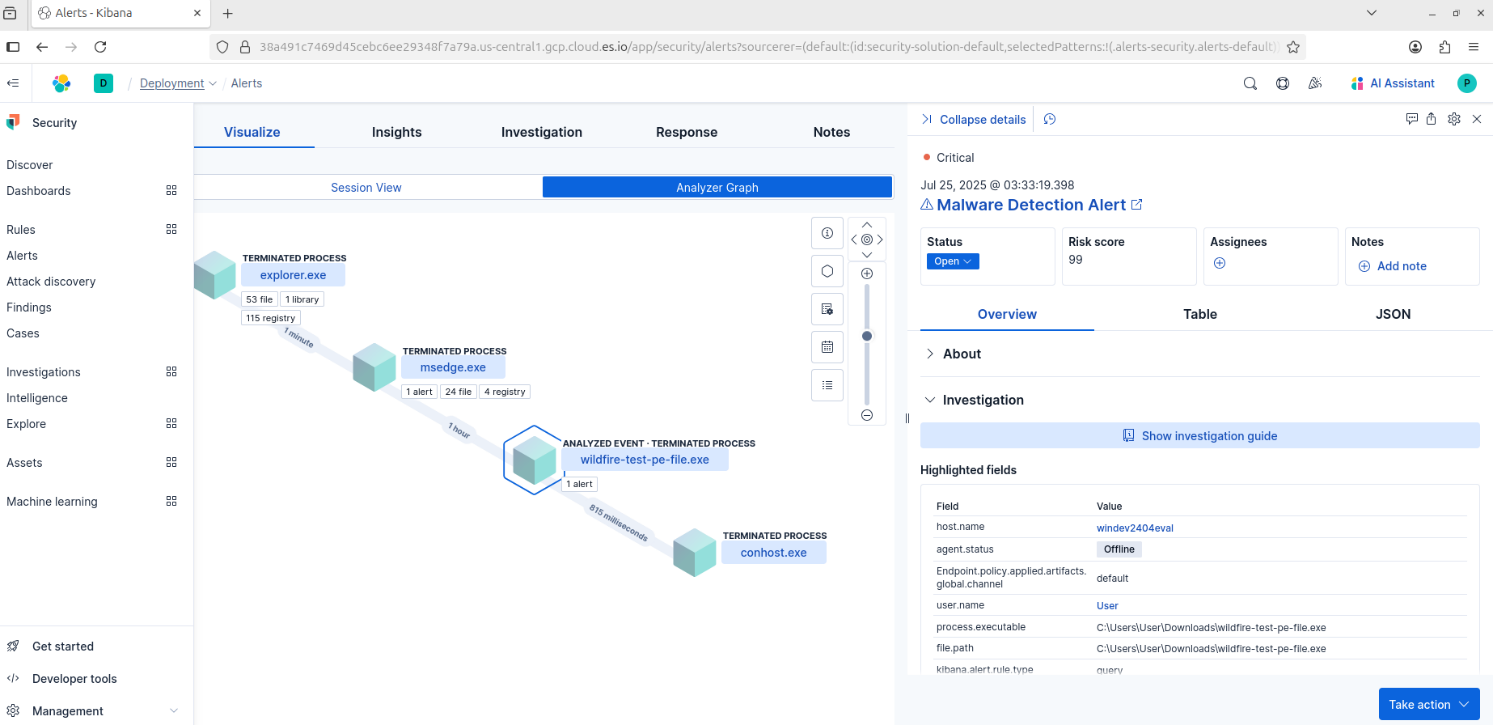
This screenshot contains the logs of the malicious file download, .exe file downloaded and the process is triggered in the windows VM and the logs are generated by zeek (network monitoring tool) and are pushed to the SIEM.



This Screenshot shows alerts in Kibana security SIEM.



This screenshot shows how the process is executed in the machine. We can see this in elastic by clicking on analyze button when the alert is generated.



This confirms that Kibana is working, zeek is monitoring the network and generating logs and alerts accordingly.