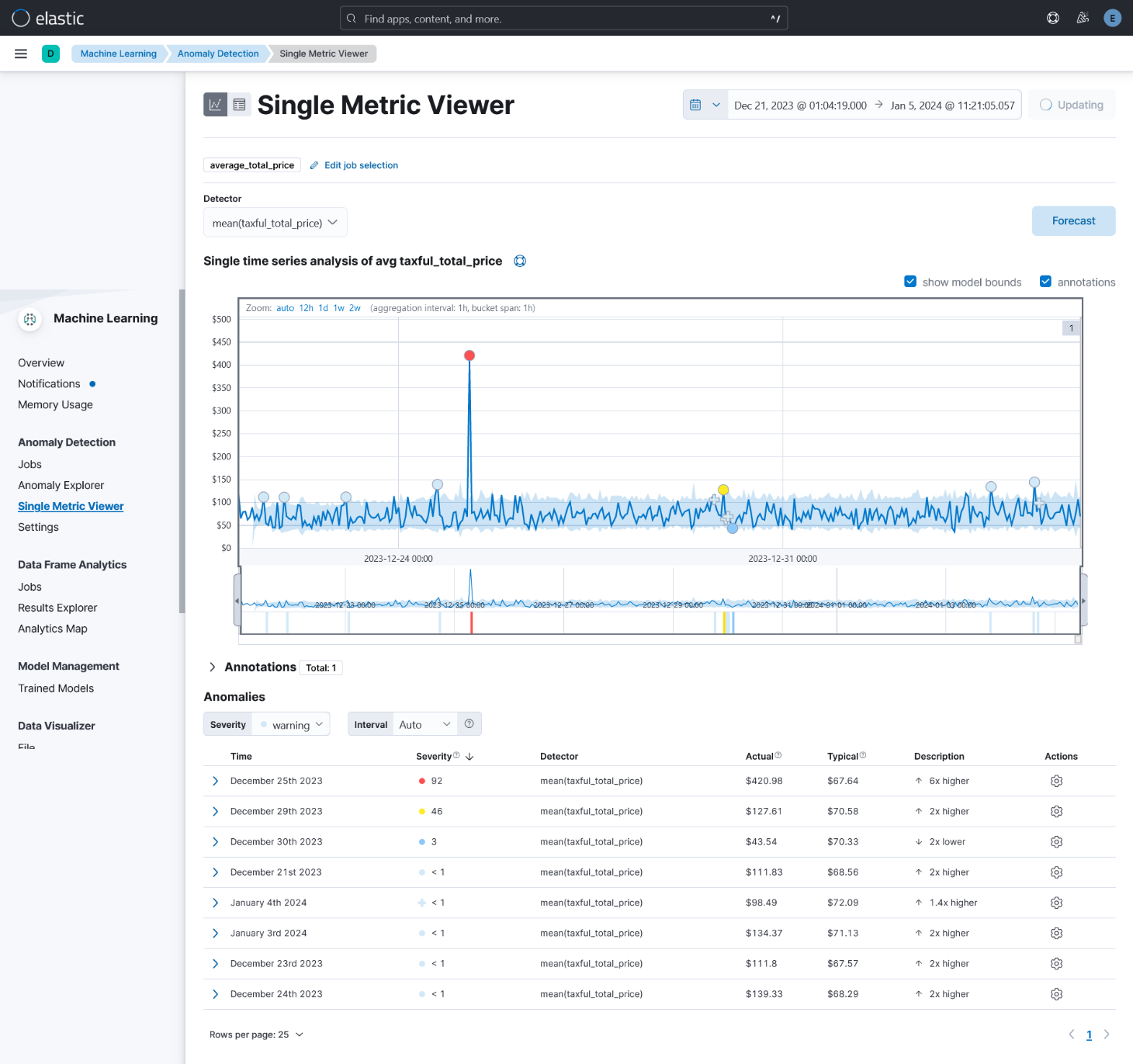
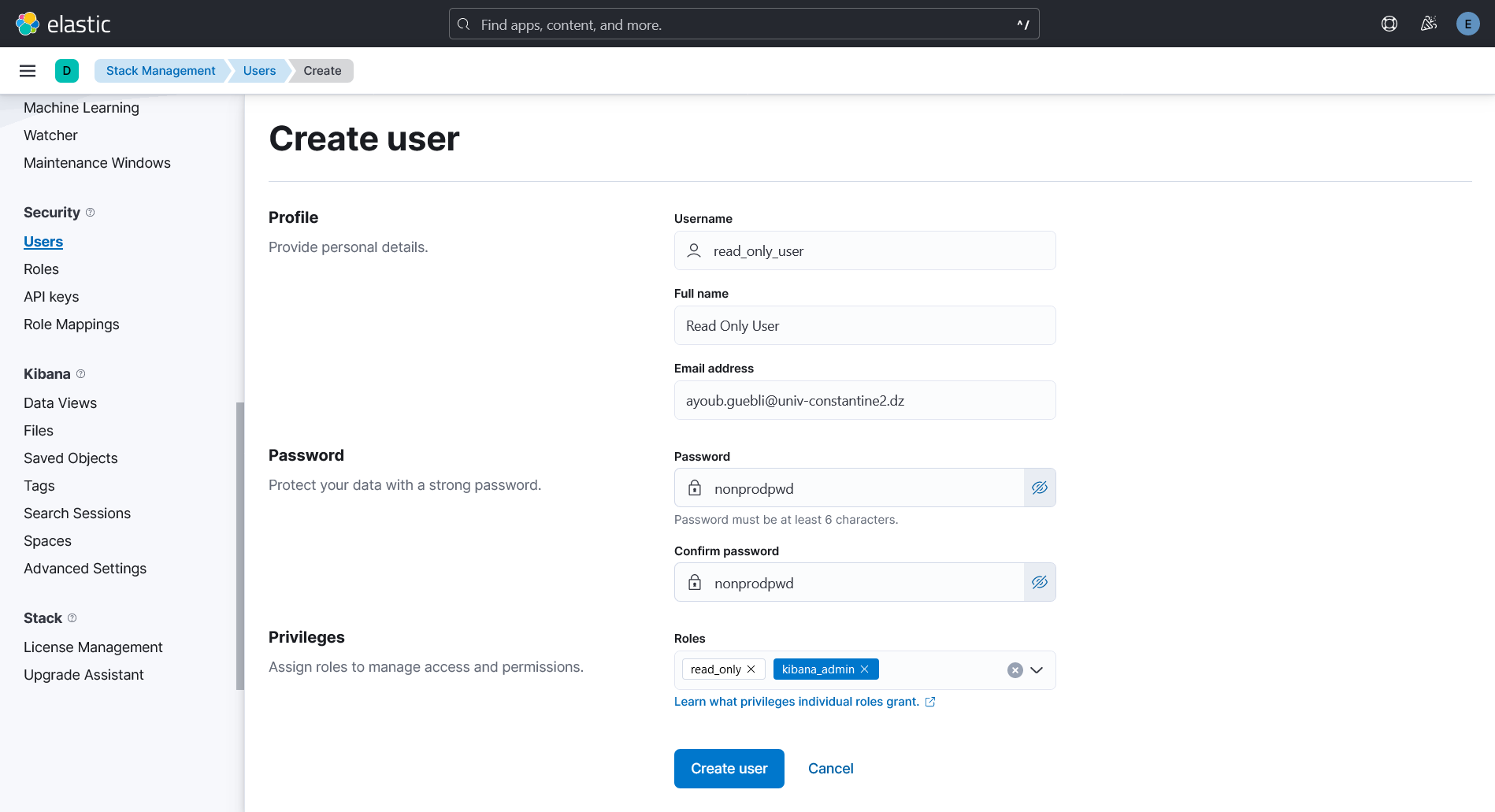
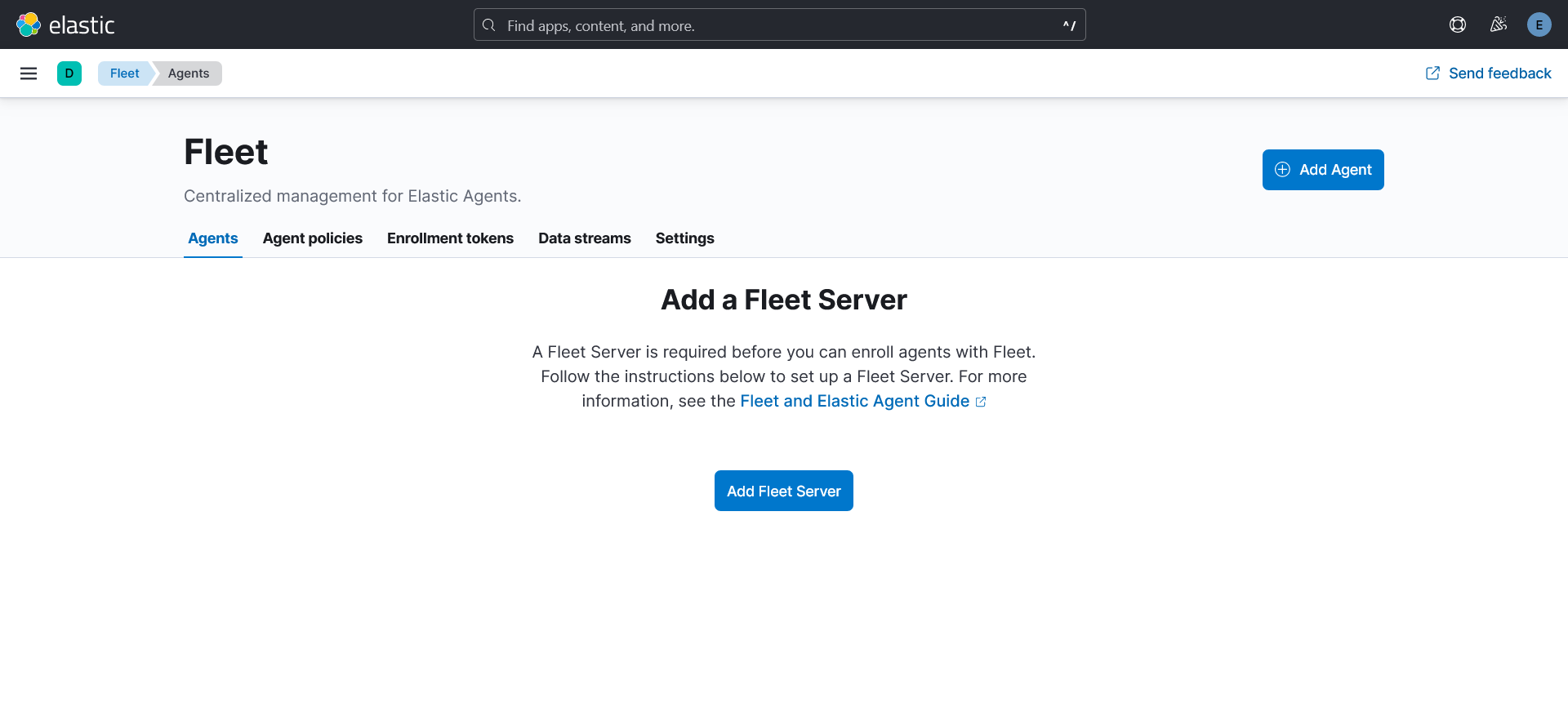
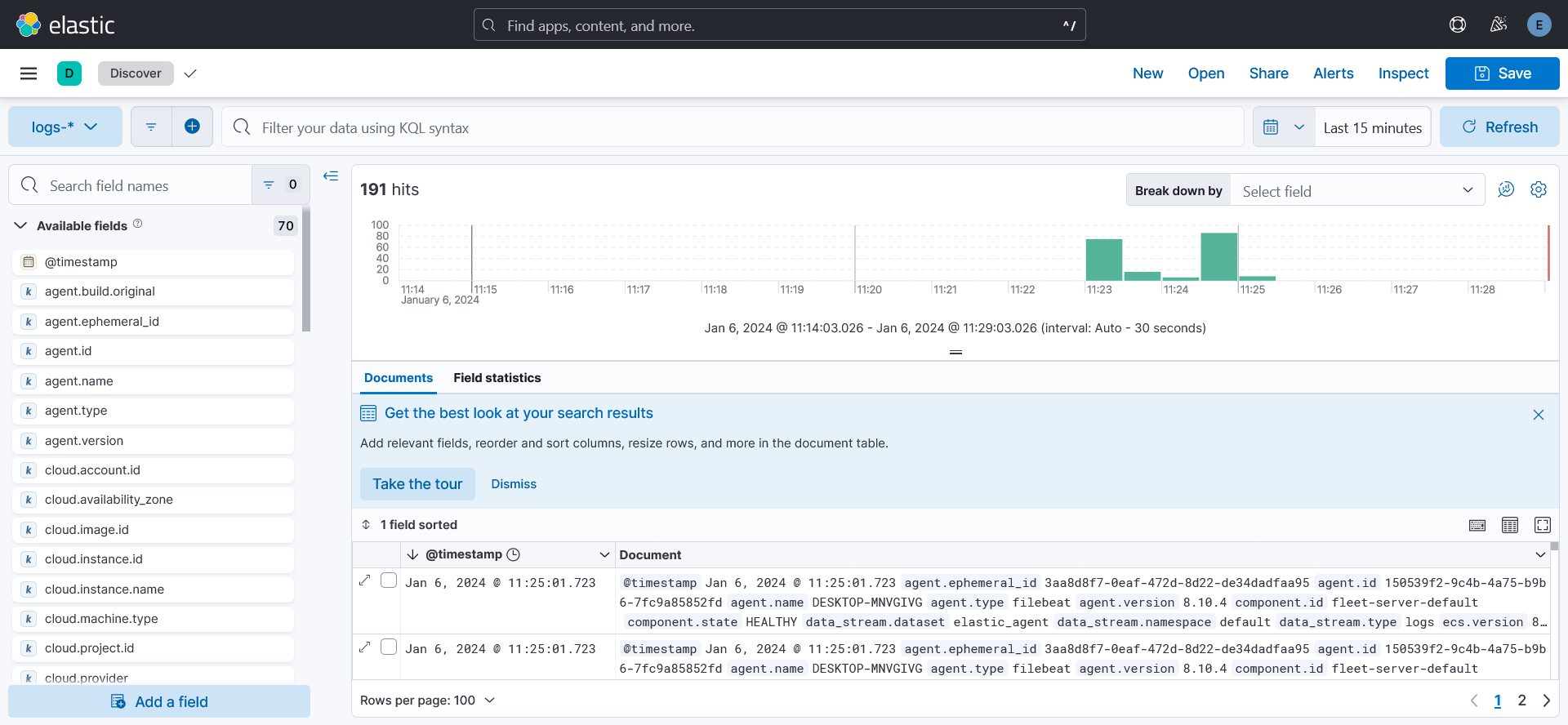
3- Create job wizard, select the kibana\_sample\_data\_ecommerce index pattern.

4-7 -If you view the earlier dates in your results, you will see two critical anomalies - they appear red in both the line graph and the table of anomalies.

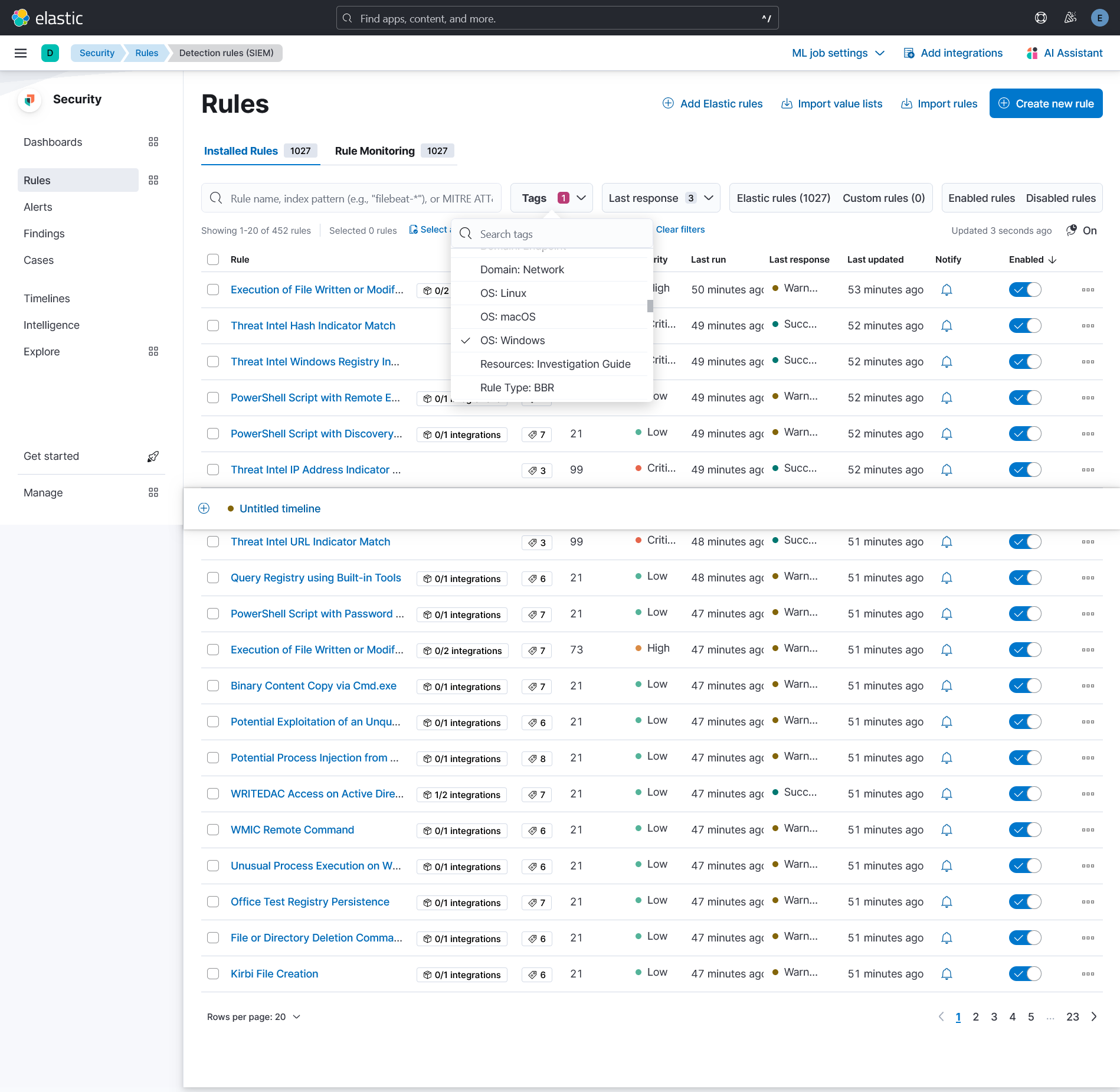
5-e- Create a new user named read\_only\_user

10-a- Under the Management heading, click on the Fleet section

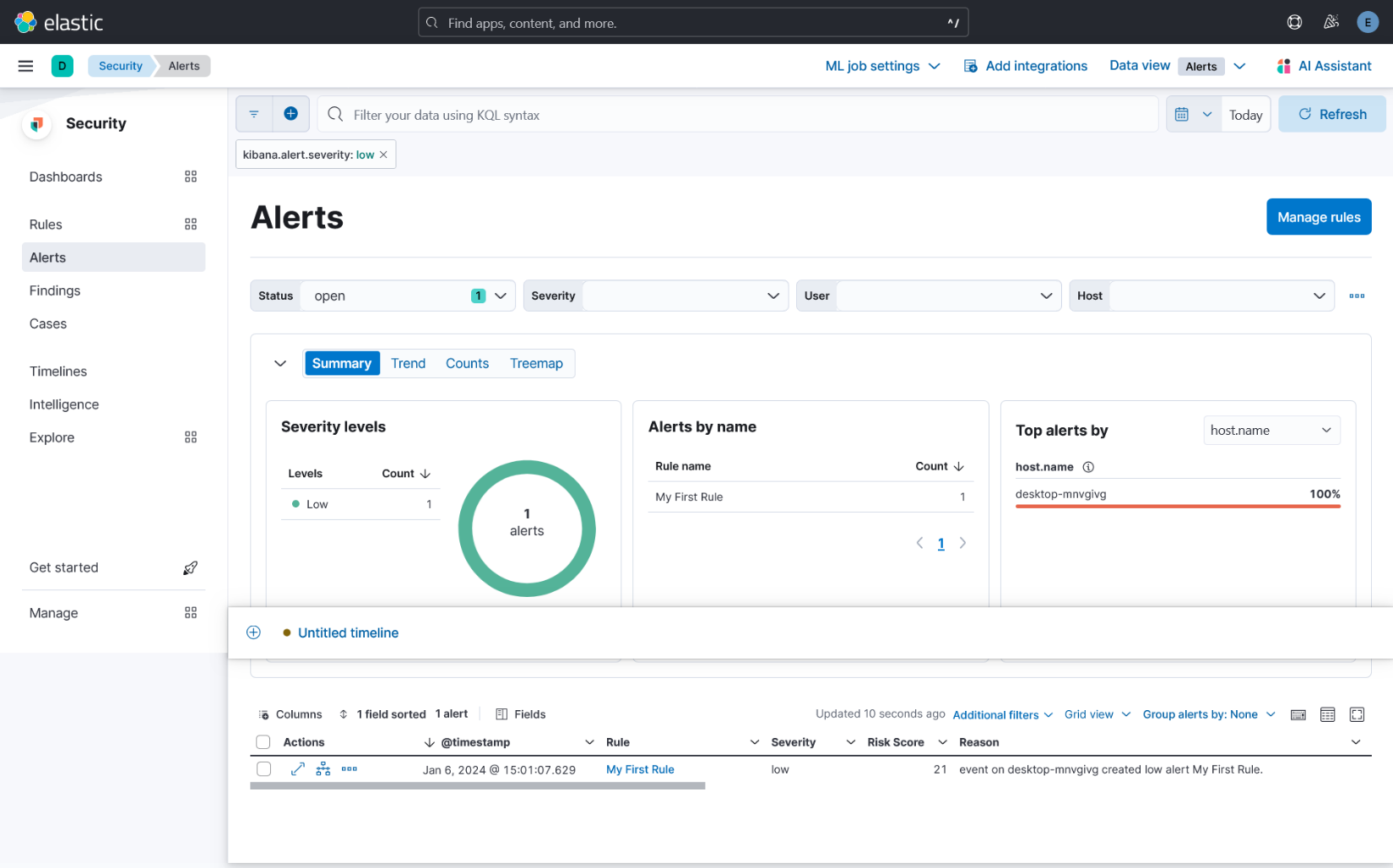
10-f- logs-\* Data view



10-h- Enable the filtered rules of windows OS:



**The Question:** as we see on the alerts table, we have 1 alert because of the rule “My First Rule”, and to see why we get this alert, we need to see this rule details, when we click on this rule,



we get the details, and we see description about this rule, “This rule helps you test and practice using alerts with Elastic Security as you get set up. It’s not a sign of threat activity “ ,so this alert was just a test ,

