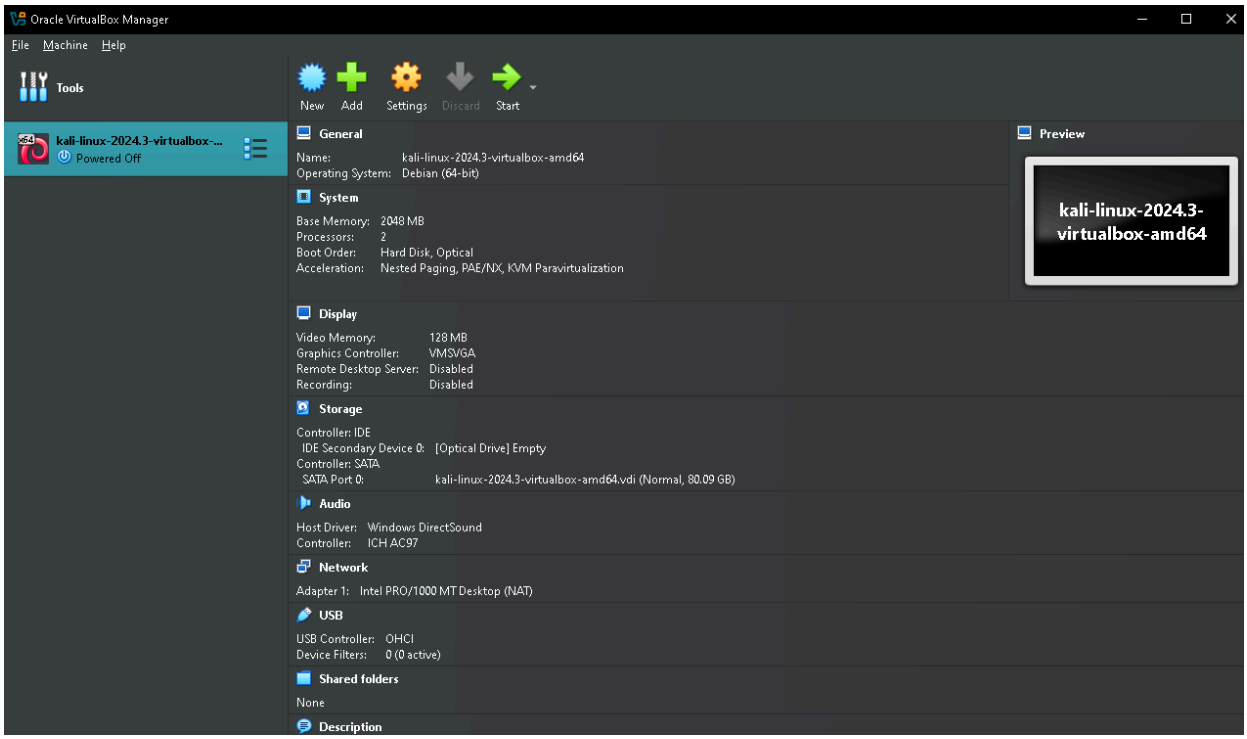
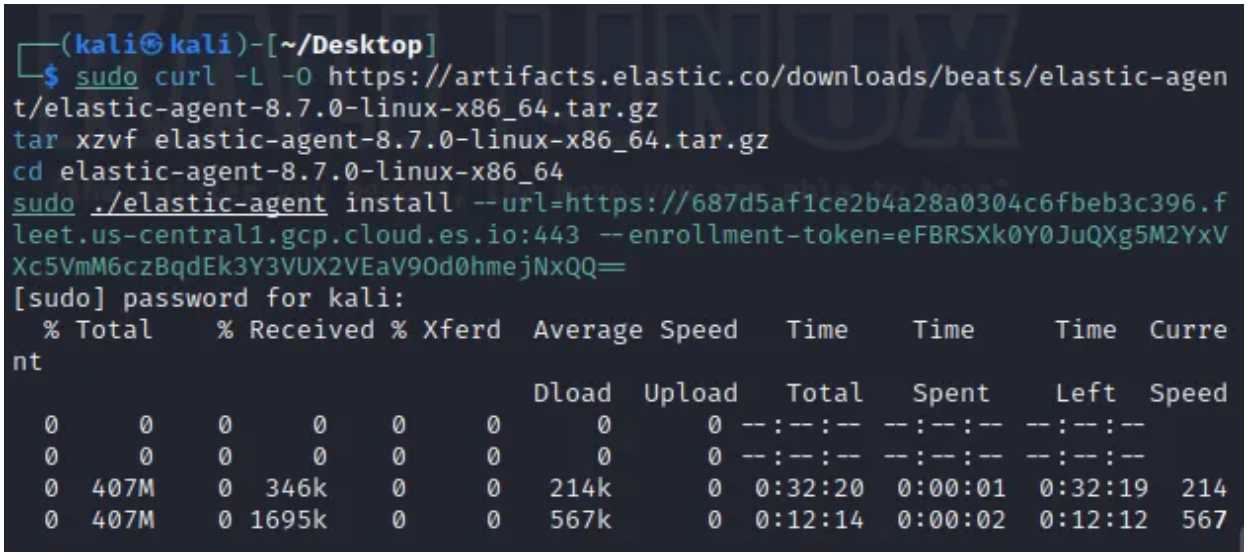
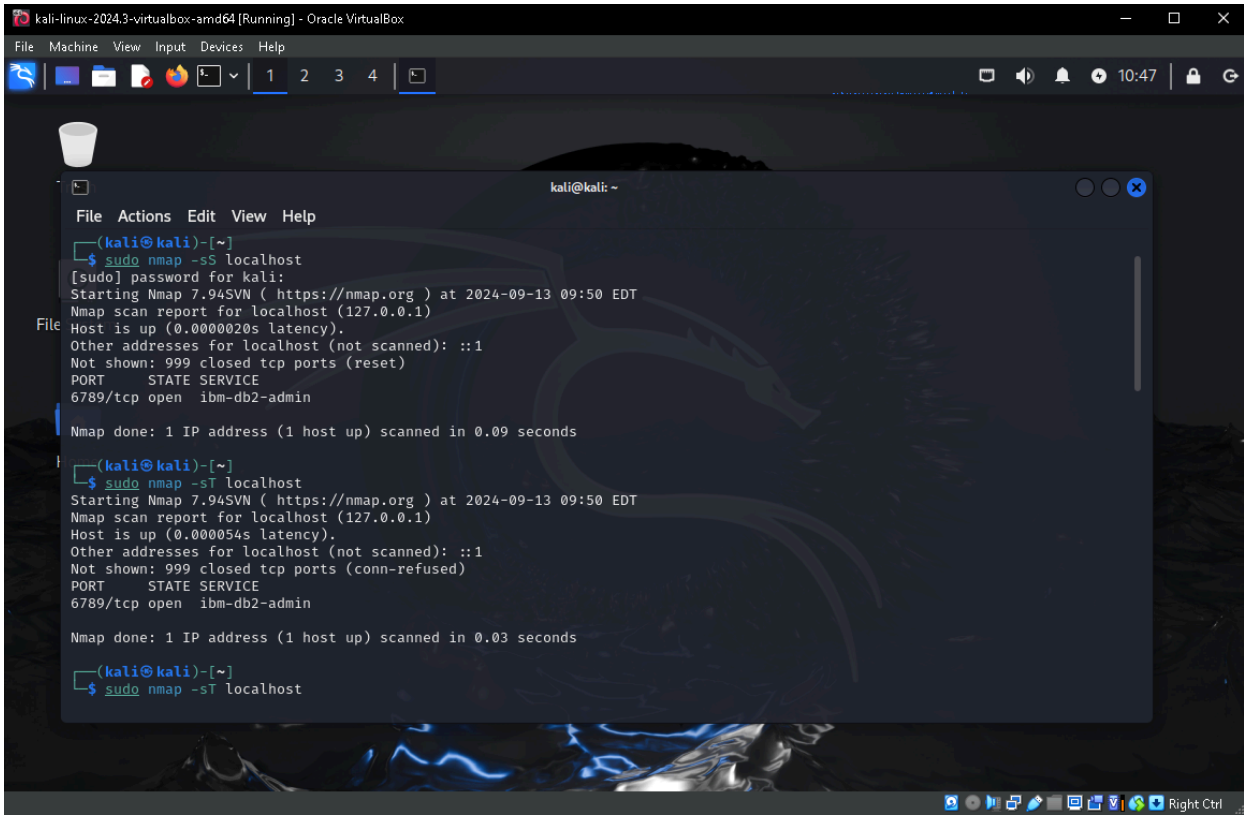
First, I installed a Kali Linux virtual machine into Oracle's VirtualBox:



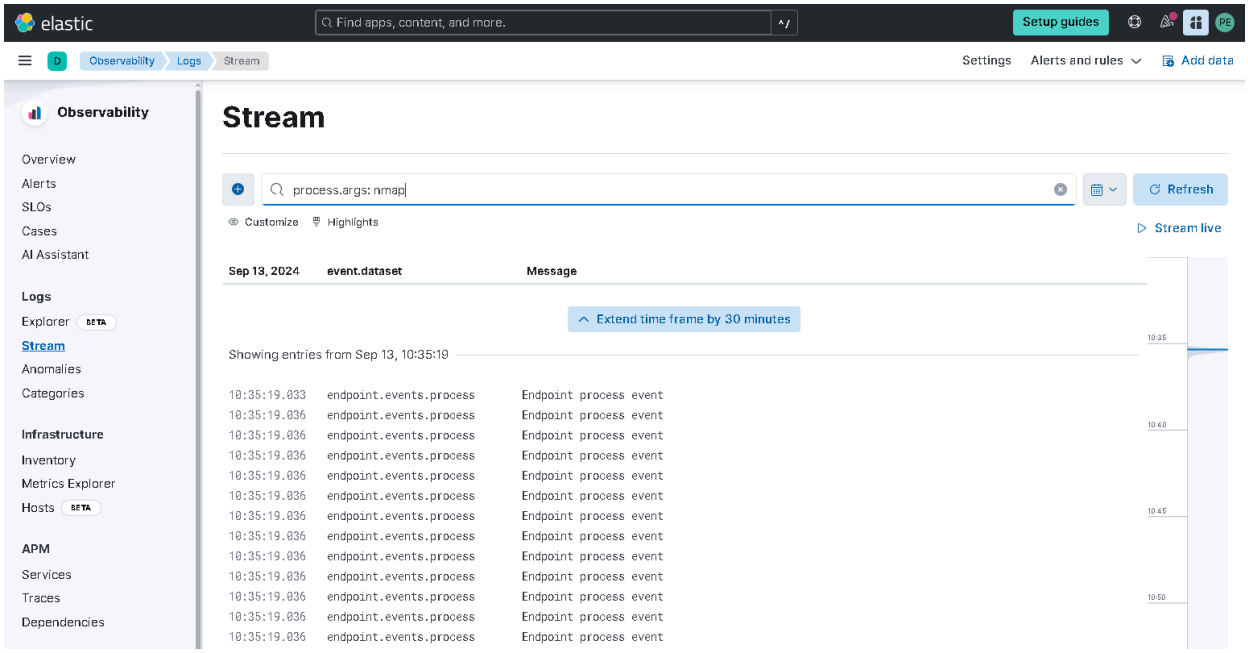
Next, I install the Elastic Cloud agent though the Kali terminal:



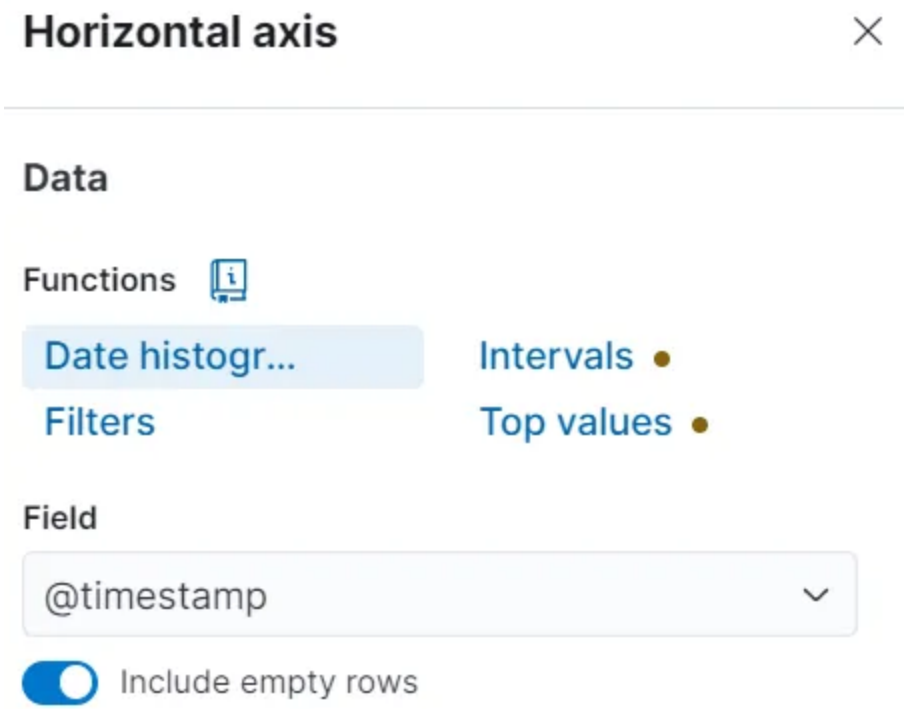
Once the agent was successfully installed, I ran a few nmap scans to generate some security events to log:

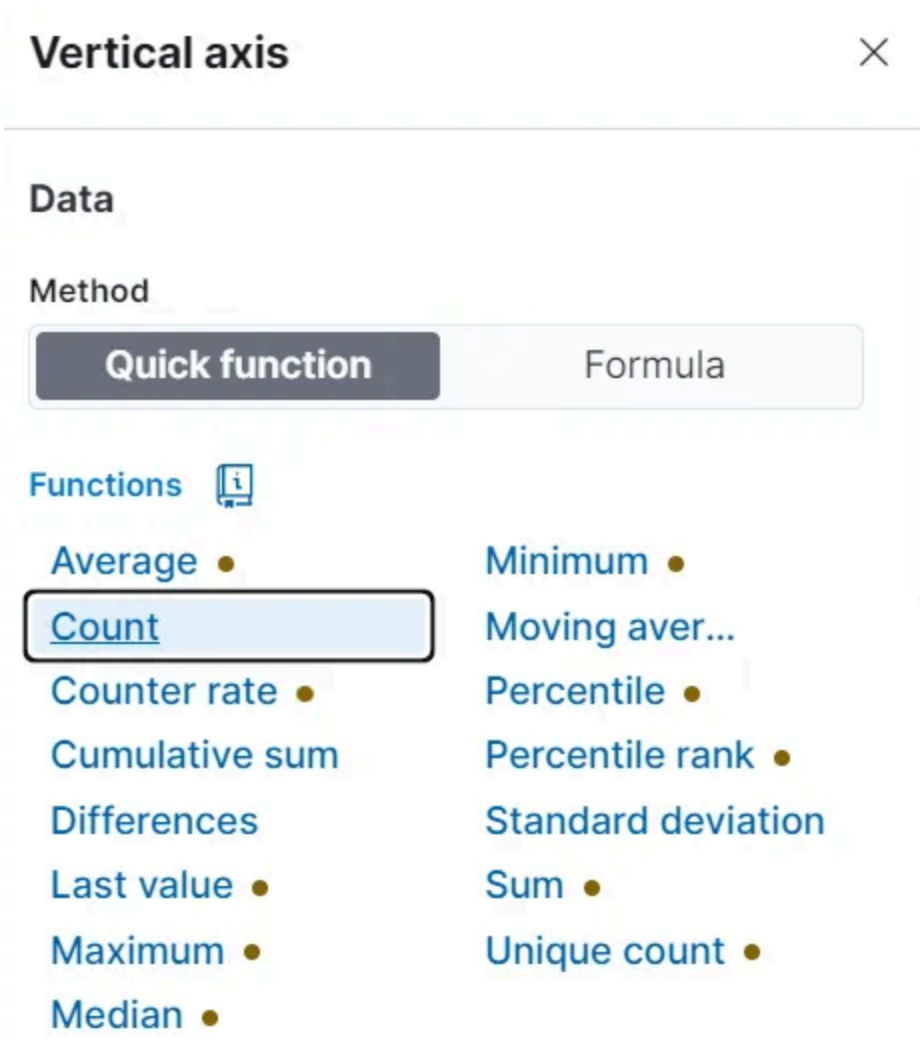


Nmap scan logs were shown here shortly after entering the search query “**process.args: nmap**” :

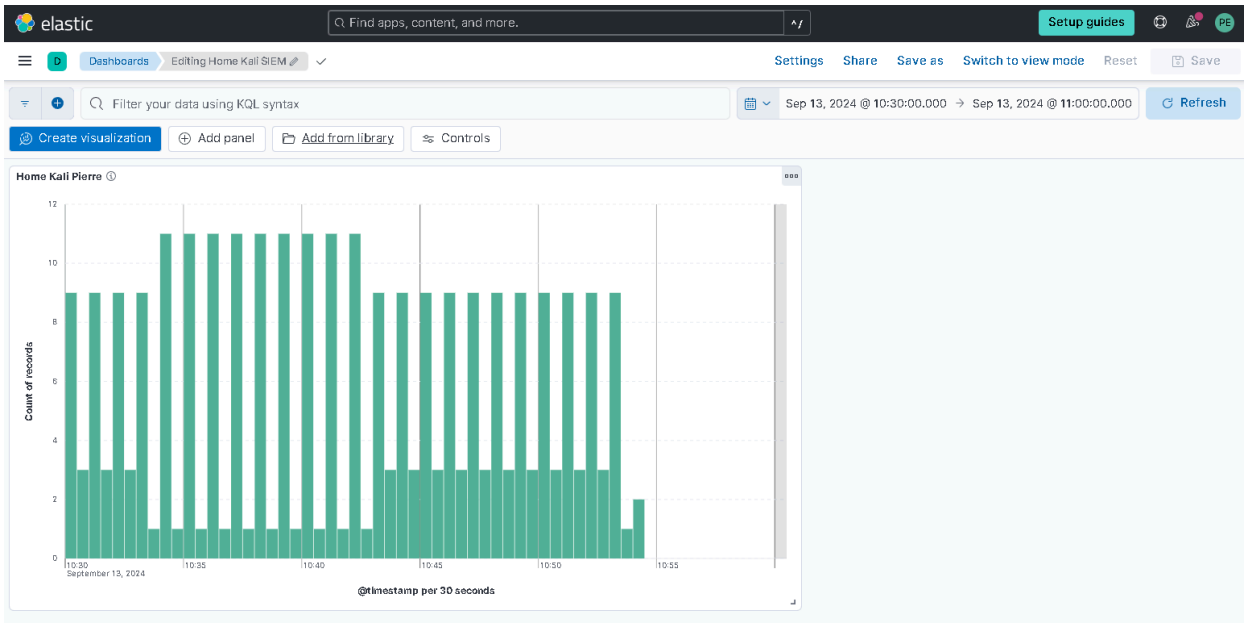


Once logs started being collected, I created a Dashboard. For the visualization, I include the Timestamp on the horizontal axis, and the count of records on the vertical axis:

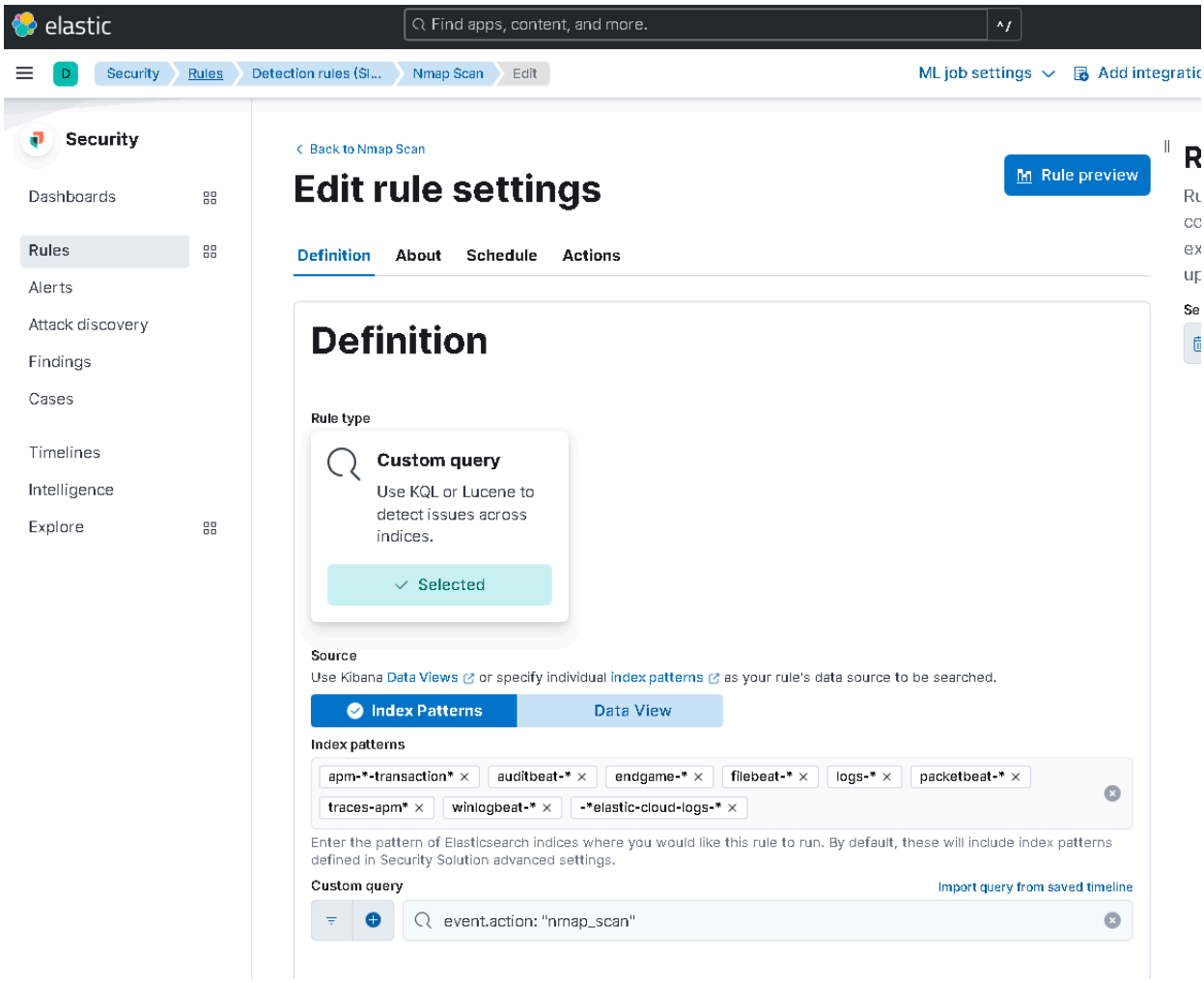

Horizontal axis
Data
Functions
Date histogr...
Intervals
Filters
Top values
Field
@timestamp
Include empty rows



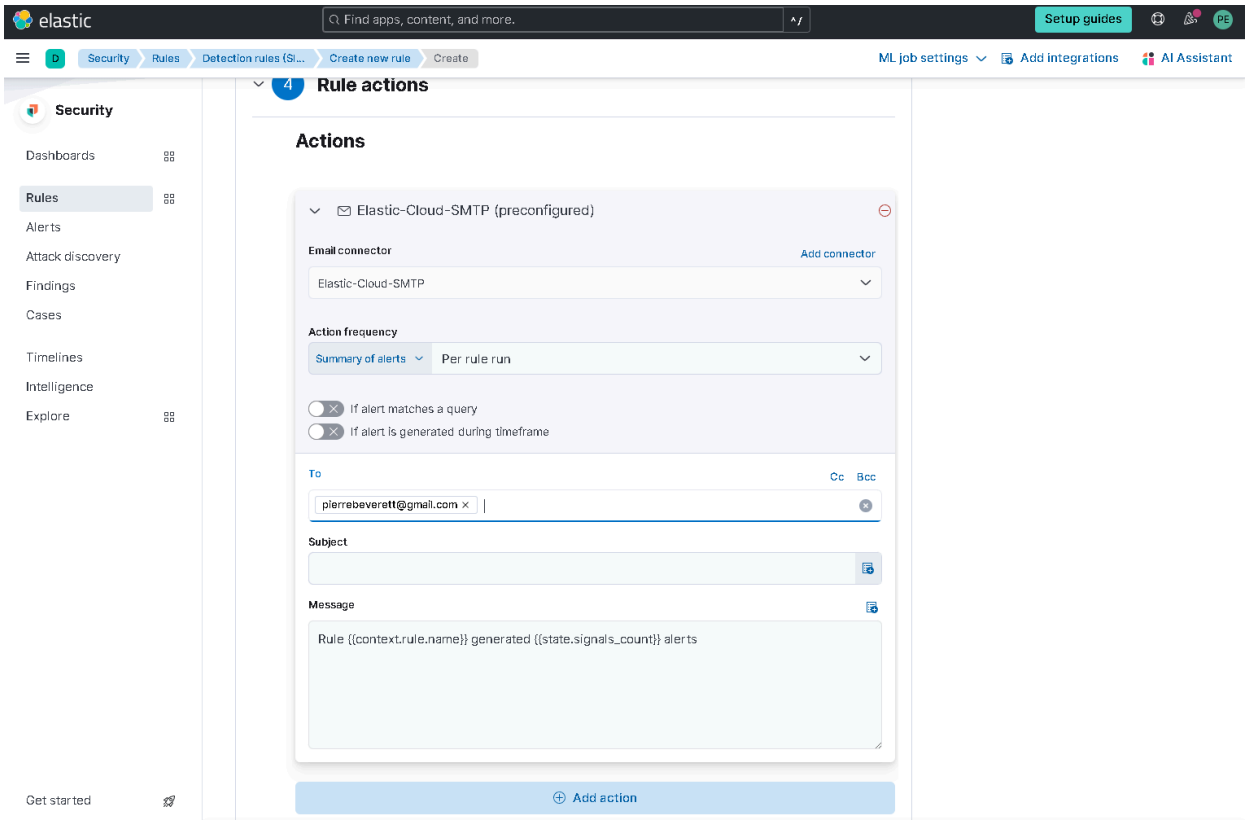
For the visualization type, I chose a bar stack, resulting in this dashboard:



Next, I start setting up an alert. Here I create a rule with a custom query **event.action: “nmap_scan”** :



Finally, I configure what action is taken when the rule is triggered. In this case, an email will be sent to the recipient:



The alert is configured and running: