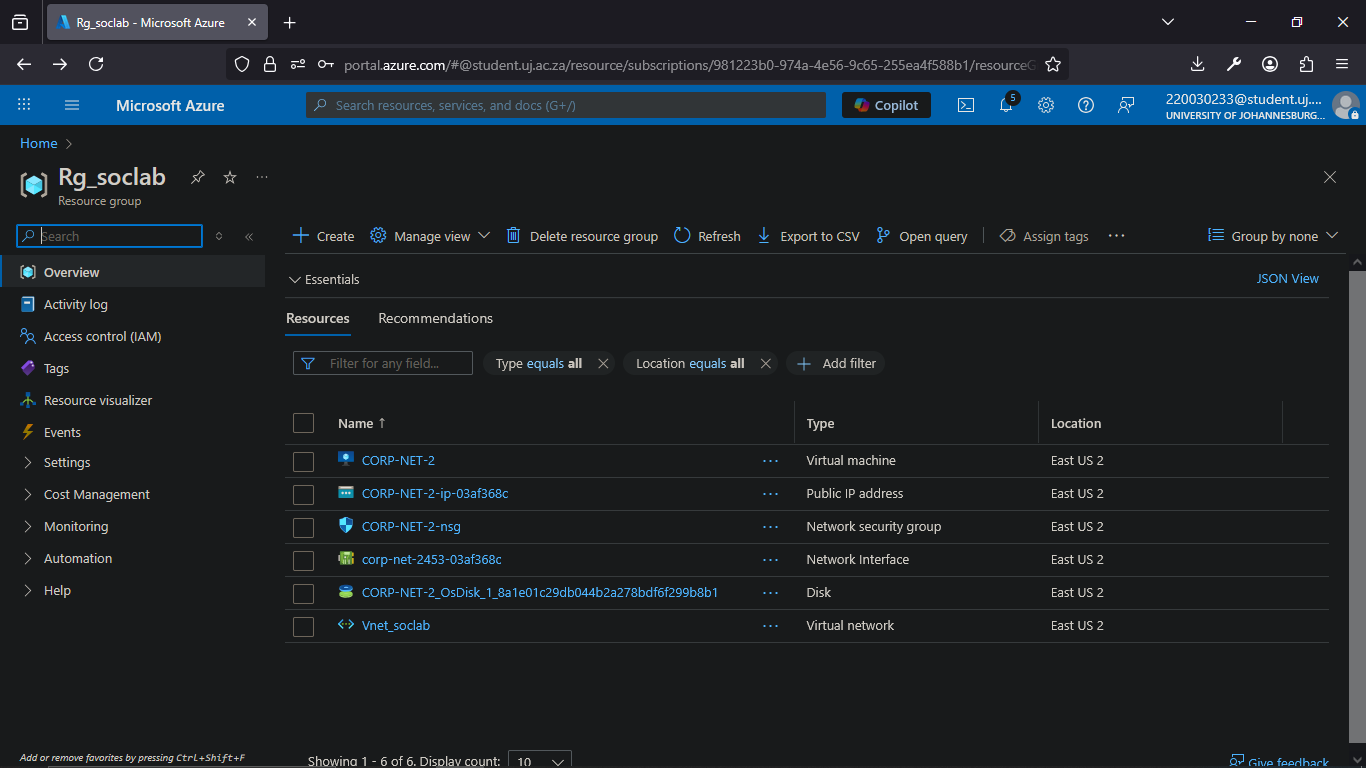
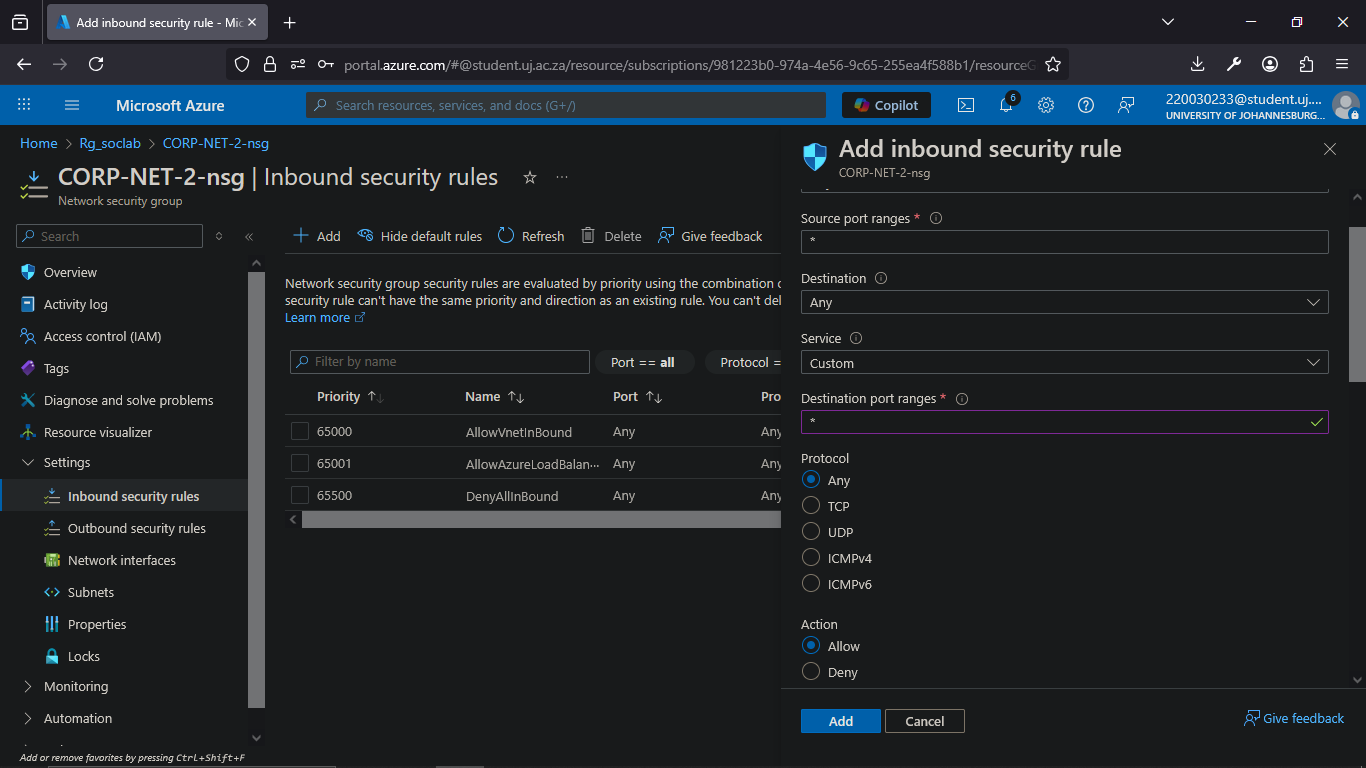


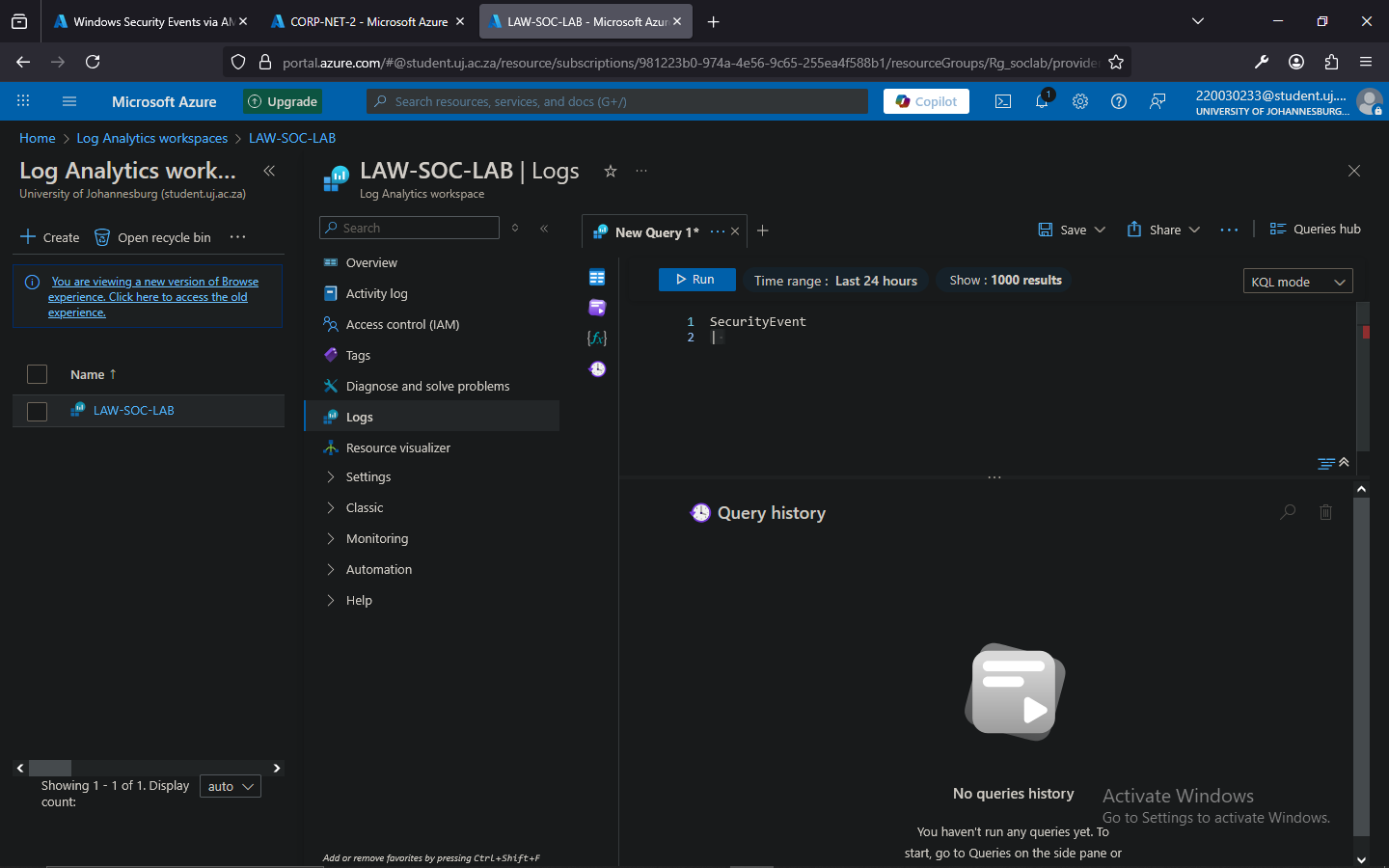
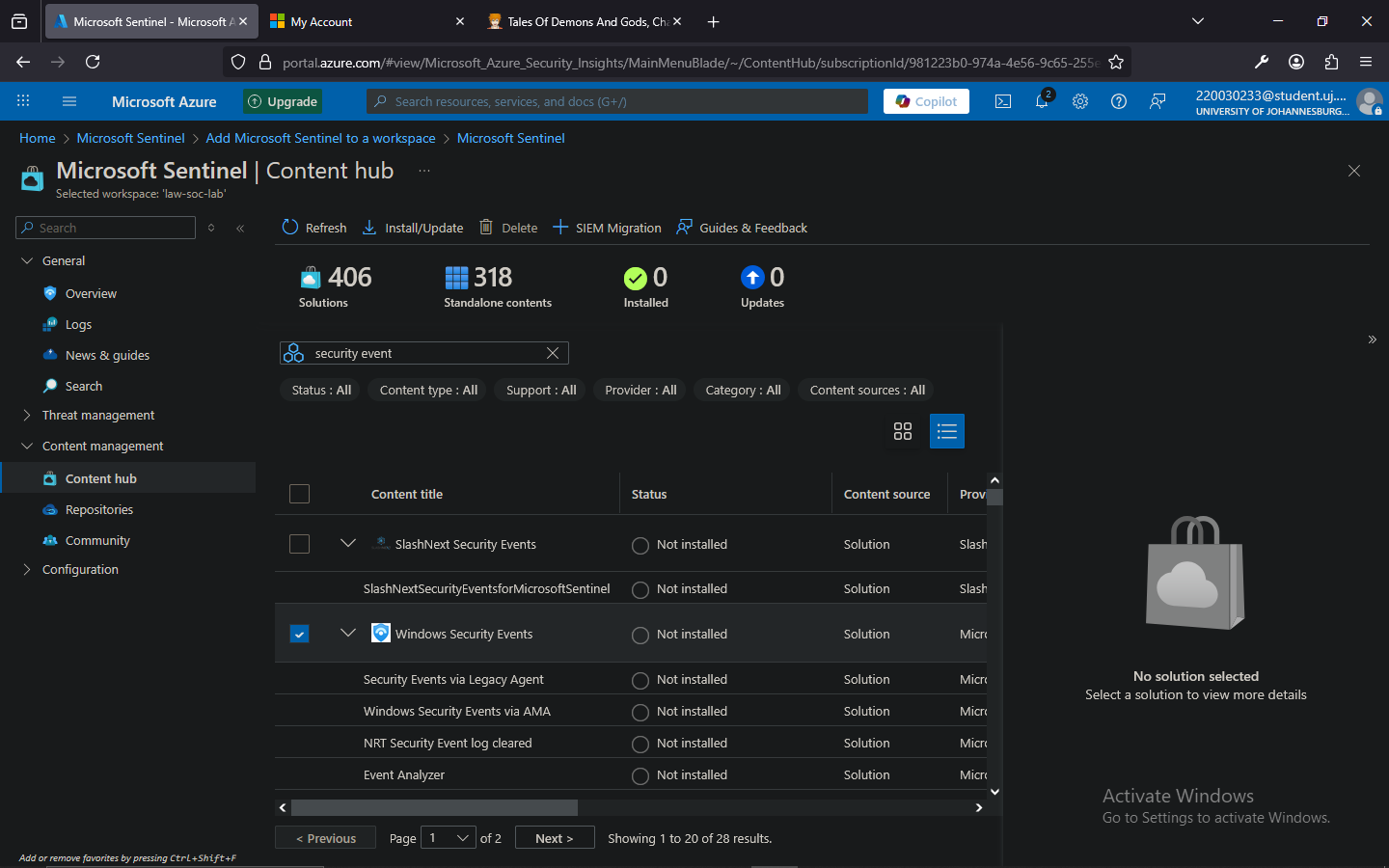
* I created an Azure account; I have my resource Group named Rg\_soclab with everything inside of it I have a virtual Network I have a subnet



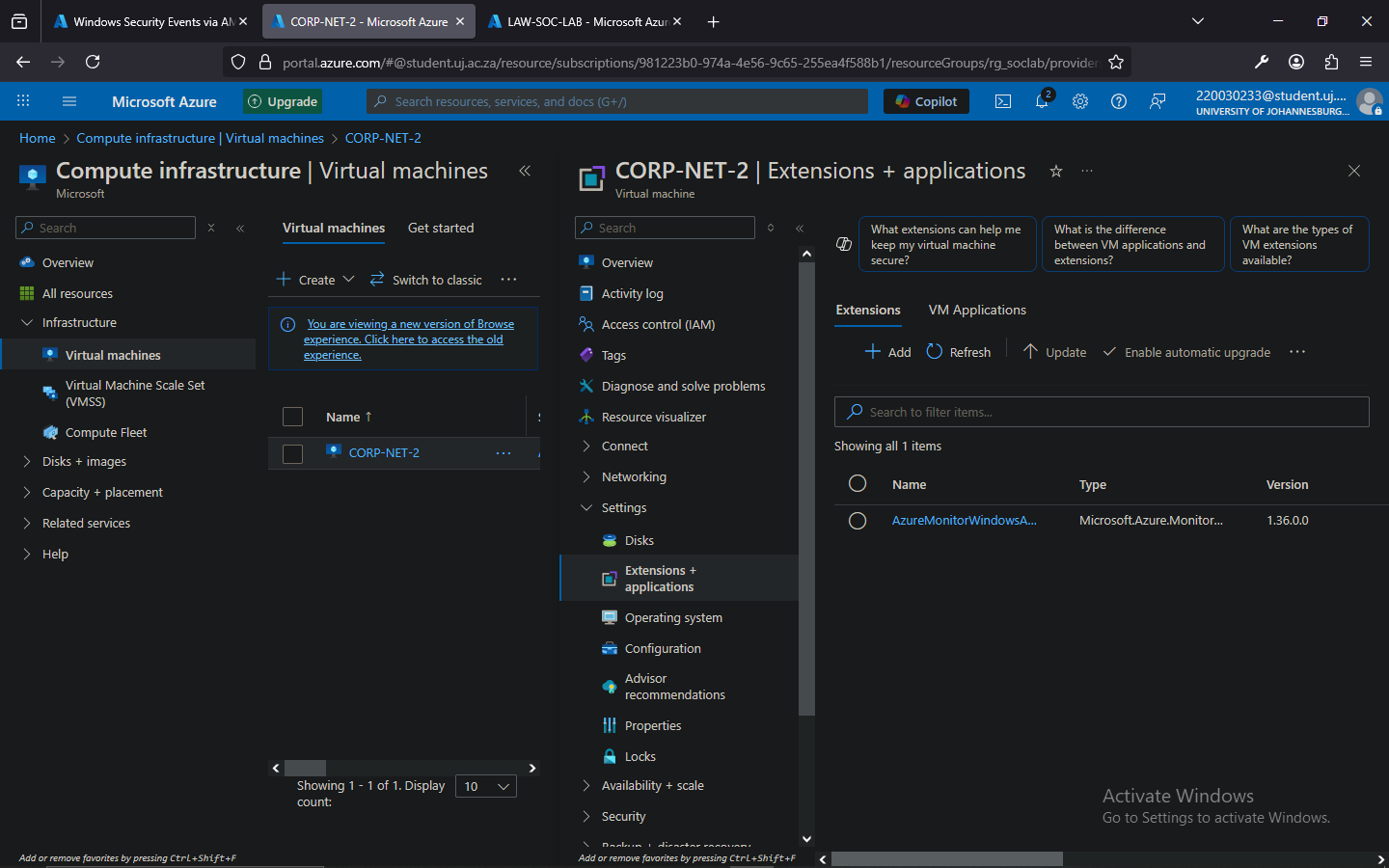
* connected to the subnet I have a virtual machine; the virtual machine's Network SEC group or Cloud firewall is completely opened to the public internet the virtual the firewall inside of the virtual machine is completely opened to the public



* I created a sentinel instance that I connected to my log analytics workspace
* inside Sentinel I uploaded a watch list which is basically just a large spreadsheet with geographic information on it with IP blocks
* I uploaded that watch list and I used the watch list in conjunction with a normal kql query to look up all the failed logins that Ire happening on my virtual machine
* I used the watch list the IP blocks and then the attacker IP address from the logs to figure out where the attackers Ire coming from around the world and then I're ultimately able to uh plot them on a map



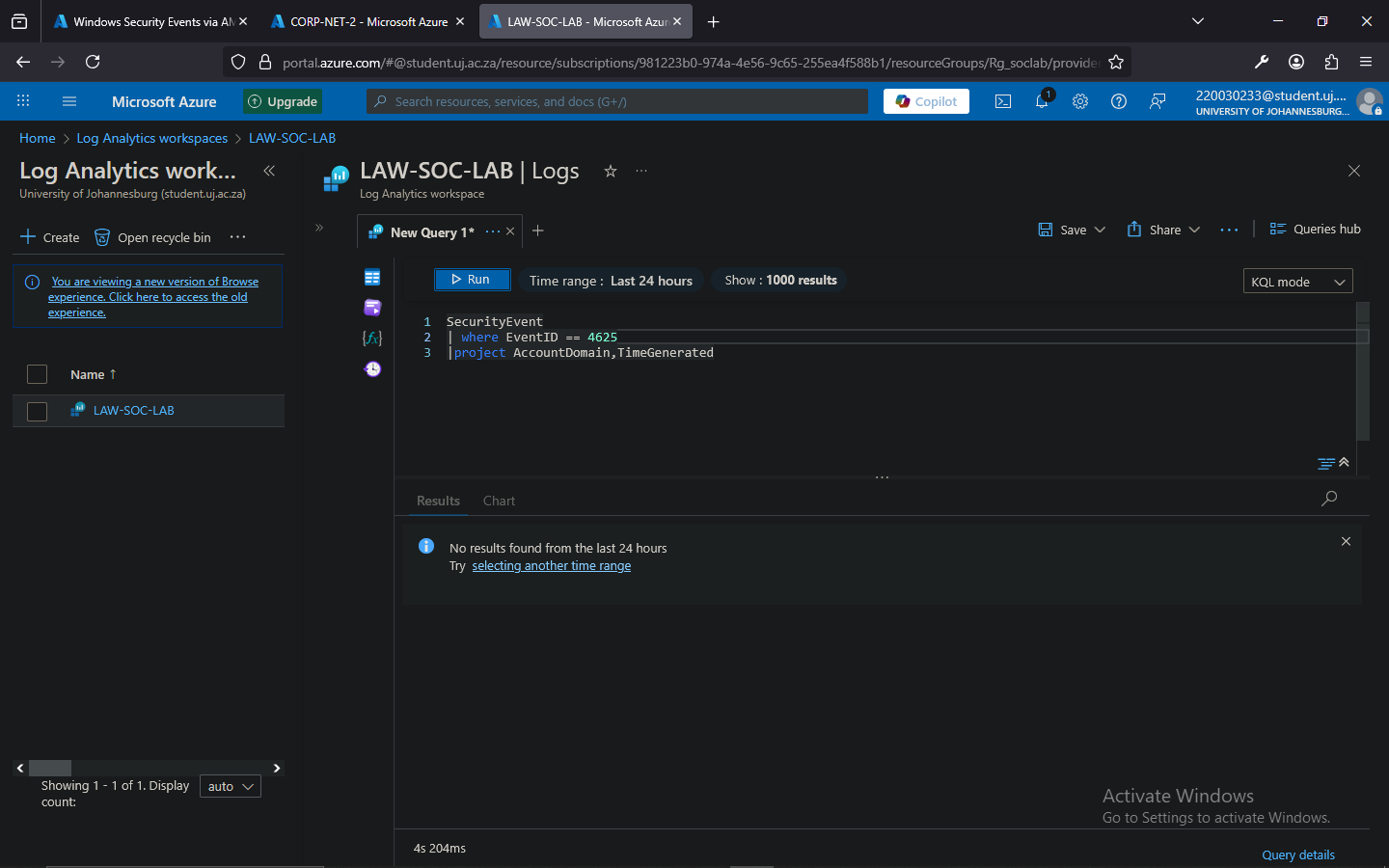
* Azure monitoring agent will forward my logs to my log analytics space

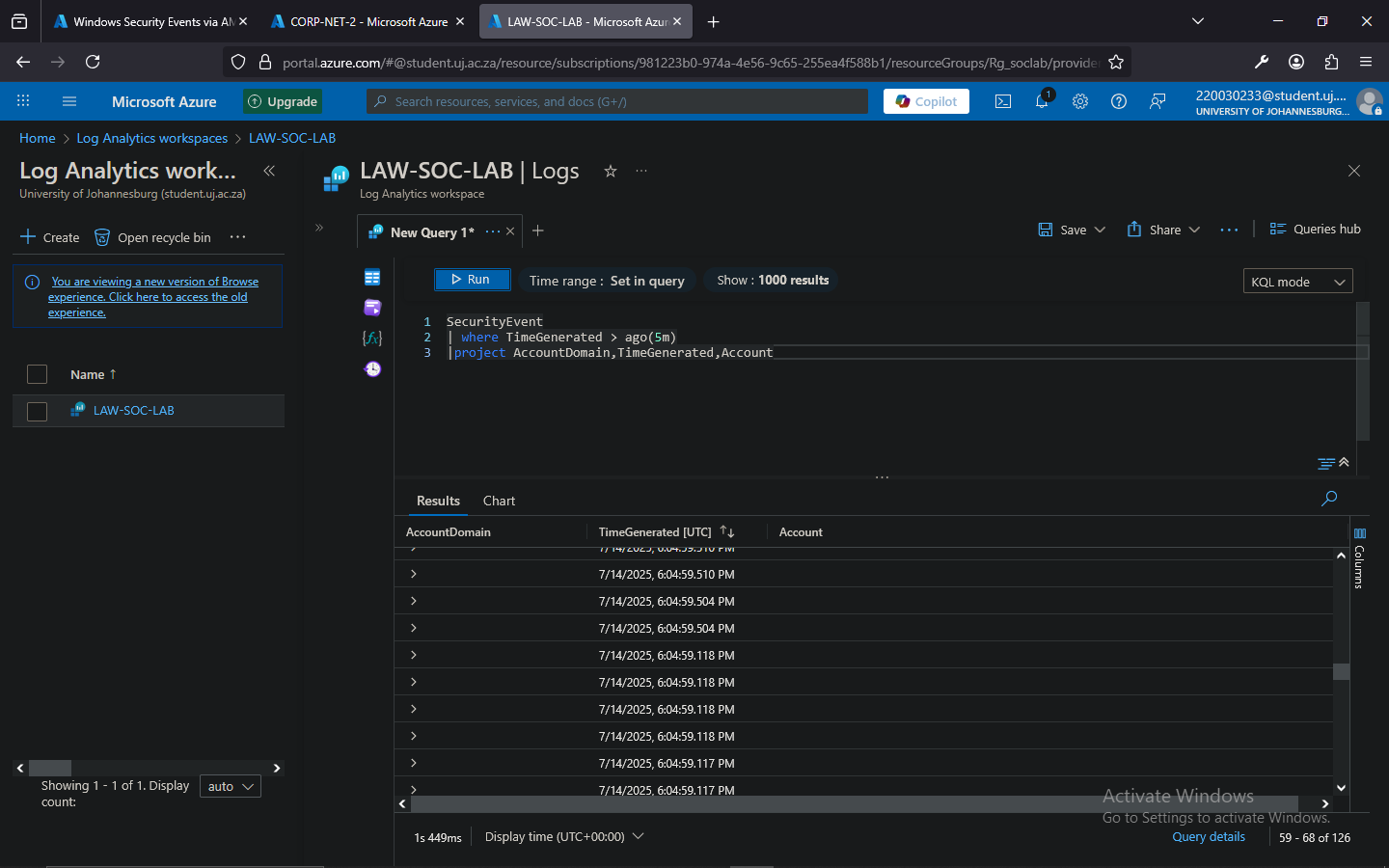


* FILTERING

A screenshot of a computer

AI-generated content may be incorrect.

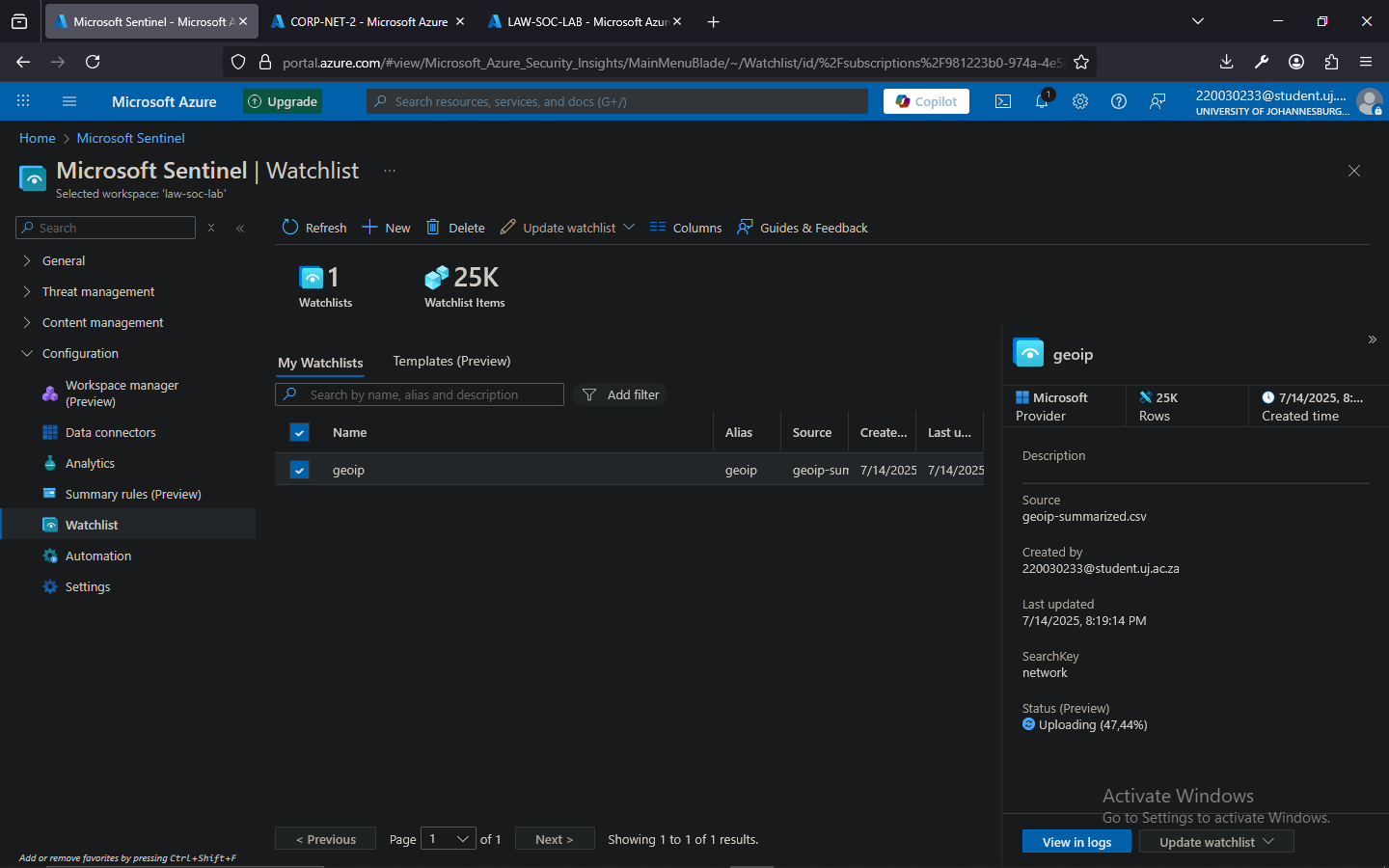




* Mapping id addresses

A screenshot of a computer

AI-generated content may be incorrect.



* My spread sheet was uploaded into sentinel, or specifically more specifically my log analytics workspace

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

* Creating map

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.