

DEMO

So, for the demo of our project, it is important to acknowledge that it is fairly automated. Once the project is established it is simply a matter of gathering logs and watching the created attack map update as long as your Virtual Machine is activated.

So, for the sake of a demo, we will show that logs are being taken using the KQL query language, and show the attack map being updated in real time.

So we are in the log analytics workspace and from here we can use this query to see any new events in any amount of time that we choose to see. We specifically target event 4625 which is the failed login event.

The screenshot shows a KQL query interface with a query editor at the top and a results table below. The query is as follows:

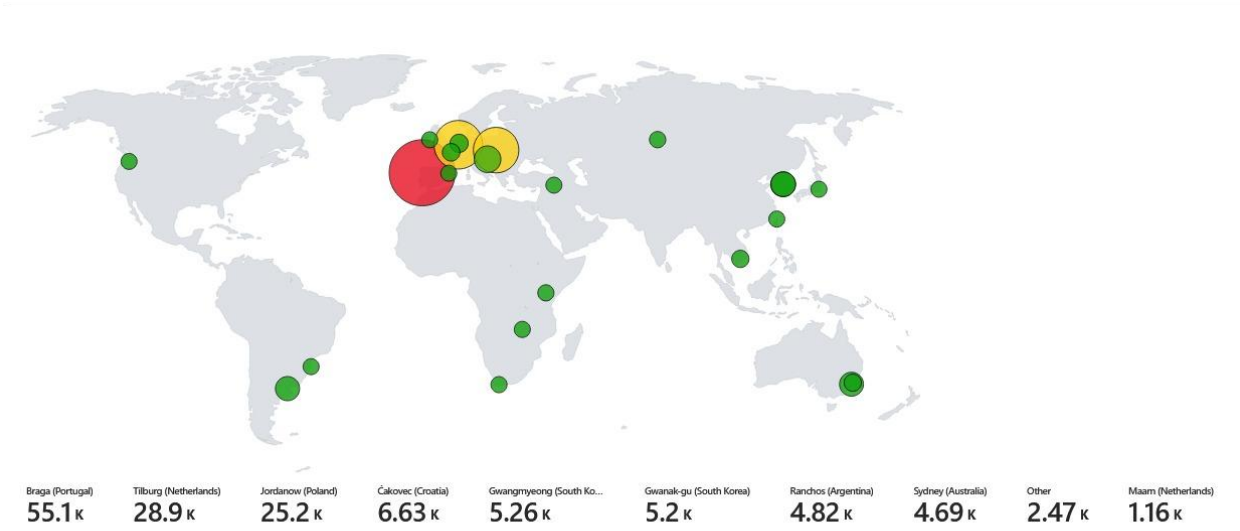
```
1 let GEOIPDB_FULL = _GetWatchlist("geoip");
2 let WindowsEvents = SecurityEvent
3   | where IPAddress == "147.93.150.115"
4   | where EventID == 4625
5   | order by TimeGenerated desc
6   | evaluate ipv4_lookup(GEOIPDB_FULL, IPAddress, network);
7 WindowsEvents
```

The results table displays the following data:

TimeGenerated [UTC] ↑↓	Computer	AttackerIP	cityname	countryname	latitude	longitude
> 11/26/2025, 7:16:27.898 AM	honey-pot-vm	147.93.150.115	Jasper	United States	35.0882	-85.5882
> 11/26/2025, 7:15:59.205 AM	honey-pot-vm	147.93.150.115	Jasper	United States	35.0882	-85.5882
> 11/26/2025, 7:15:54.905 AM	honey-pot-vm	147.93.150.115	Jasper	United States	35.0882	-85.5882
> 11/26/2025, 7:15:26.328 AM	honey-pot-vm	147.93.150.115	Jasper	United States	35.0882	-85.5882
> 11/26/2025, 7:15:22.039 AM	honey-pot-vm	147.93.150.115	Jasper	United States	35.0882	-85.5882
> 11/26/2025, 7:14:53.867 AM	honey-pot-vm	147.93.150.115	Jasper	United States	35.0882	-85.5882
> 11/26/2025, 7:14:49.150 AM	honey-pot-vm	147.93.150.115	Jasper	United States	35.0882	-85.5882
> 11/26/2025, 7:14:26.684 AM	honey-pot-vm	147.93.150.115	Jasper	United States	35.0882	-85.5882
> 11/26/2025, 7:14:17.852 AM	honey-pot-vm	147.93.150.115	Jasper	United States	35.0882	-85.5882

At the bottom of the interface, it shows a performance metric of 1s 73ms, a display time setting of (UTC+00:00), a link to 'Query details', and a pagination indicator '1 - 10 of 1000'.

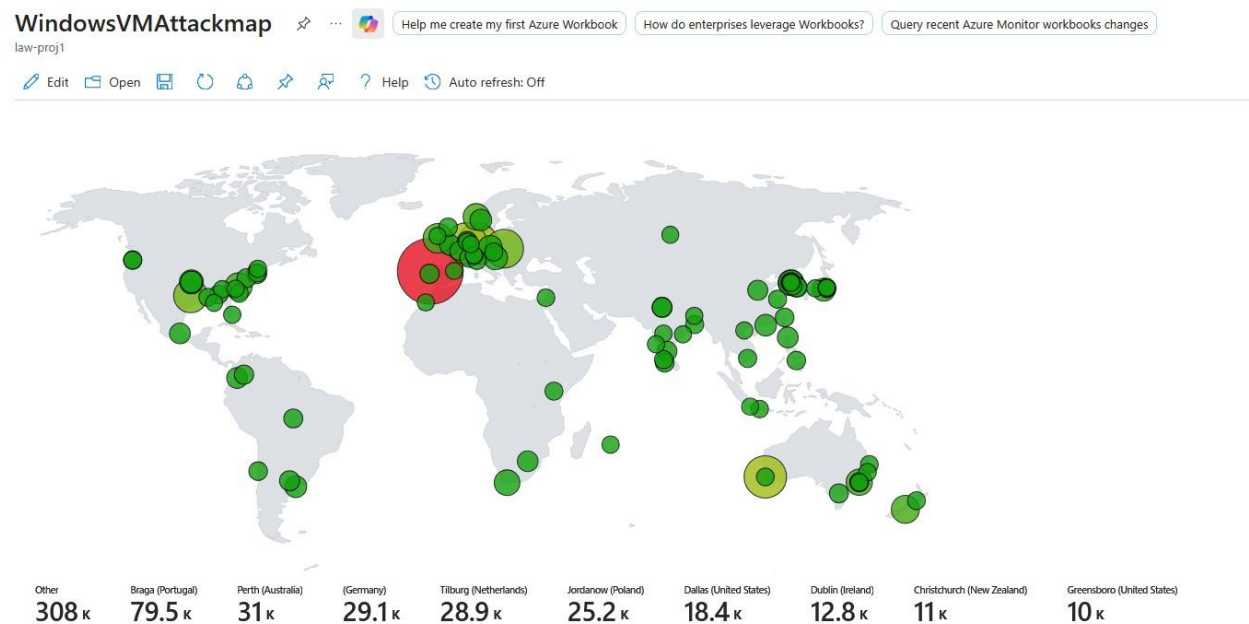
Going into Sentinel, you can access the created attack map by going to the Workbook section. From there, we can see the map and see logs updating in real time. The map updates on its own but we can force update it. To show it being updated, here is the map increasing in logs over time.



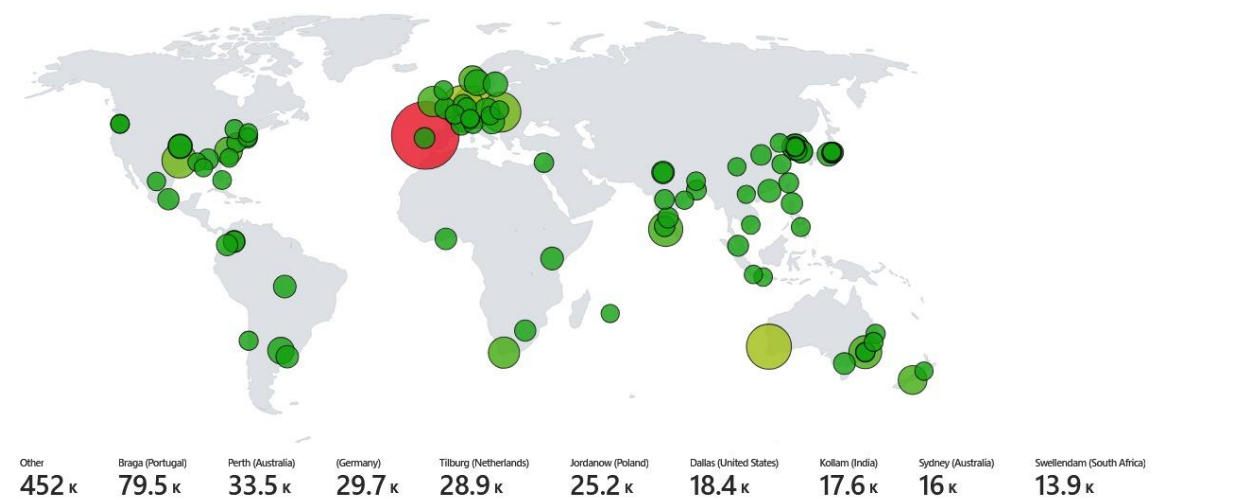
2 weeks later



About 1 week later.



Last week before the free trial ended.



So I hope this served as an adequate demo of our project. As you can see logs are still being processed and reflected in the attack map. Thank you.