

Wishlist/Shortcomings

When constructing this project we had a number of limitations and shortcomings we wish we could have tackled. When it came to limitations, it was a matter of finance. Azure is subscription based and if we were not careful, we would get charged harshly to do certain things.

Some may wonder why use proprietary software instead of using only open-source solutions, and the answer to that comes from safety assurance. This type of project can be dangerous if you do not know what you are doing, so using Azure, a cloud-based solution, made it easier to not only rationalize, but also gave us some peace of mind.

Another limitation was timeframe, Azure, and more specifically Sentinel only allowed up to 30 days of data logging, so once that was over, our data collection would cease and effectively break the map, so time management was key.

Any improvements that could be made revolve more around scale. It would have been nice to have multiple VM instances run and collect logs. Another was the possibility of creating attack maps for different security events. While monitoring the logs, we noticed some users actually managed to log in to the VM, and changed permissions, so it would have been interesting to see it either in an attack map or some kind of pie chart.

Regardless, the team is satisfied with the result and acquired a lot of interesting data to look at. We received millions of total logs from all over the world. And feel we caught a pretty good glimpse into how integral SIEMs are for maintaining strong cybersecurity.