Contribution ID: **21** Type: **Presentation (25 minutes)**

Using an analytical database to augment nfdump/nfsen

Wednesday, 10 April 2024 11:00 (20 minutes)

nfdump/nfsen are a great set of tools for analysing netflow based network data, both for network management and for cybersecurity purposes. The biggest drawback for security applications is that finding IoC occurrences for any sensible timeframe (e.g. up to two weeks back) will take hours, if not days. Rather than trying to replace nfdump/nfsen, a better approach is to address only this specific deficiency with other tooling, such as an analytical database, which are designed to run queries over large volumes of data quickly. The results of these queries then help with using nfsen for further detailed analysis. In this presentation I will address how we implemented this at SURF and have been running it successfully for over a year. I will also show how the analytical database can be used for other purposes, such as continuously monitoring incoming network data for occurrences of IoCs based on a curated MISP feed.

I hope the audience take away the idea that different tools can augment each other and there is no need to look for a perfect solution that does everything. (Also that analytical databases are awesome and better in most cases than Big Data approaches)

Primary author: POORTINGA, Remco (SURF)

Presenter: POORTINGA, Remco (SURF)

Session Classification: Technical Deep Dive

Track Classification: Presentation