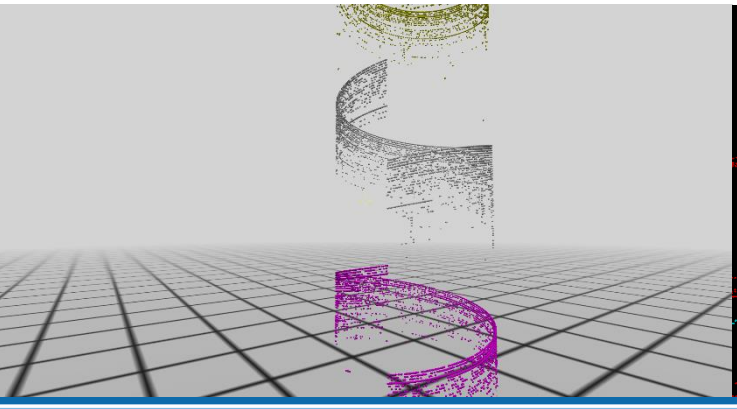
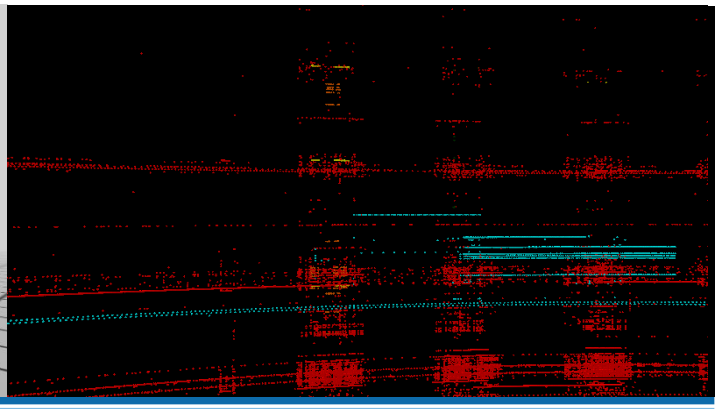
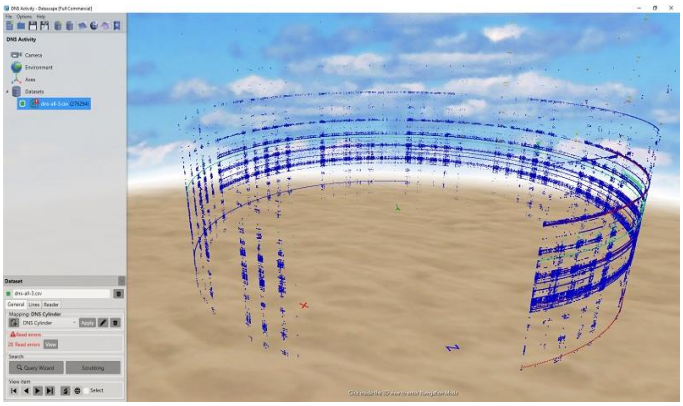
Cyber-Security Data

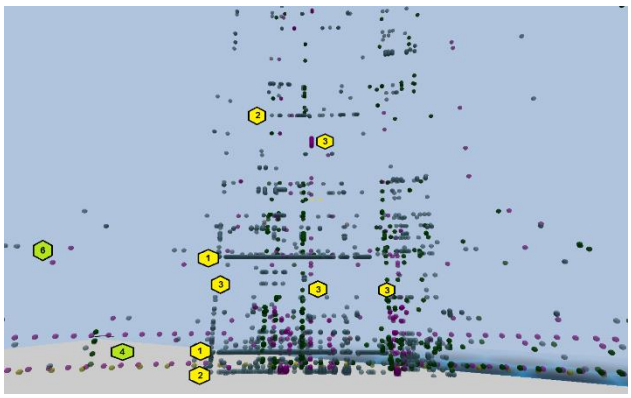
3D Visualisation of network DNS requests





As part of a Centre for Defence Enterprise project Daden worked with cyber-security experts Assuria to investigate different ways of visualising different types of cyber data. One particular dataset was the log of DNS activity on the network. Whilst one would have expected that each web page request from a user would result in a single DNS call, and that activity would be limited to working hours, the reality was very different.





The Cylinder

The log data included about 800,000 events covering about 12 weeks of monitoring. Trying to see all this data in one go, and be able to maintain context whilst zooming in and out is a real challenge in 2D. In 3D we found that a cylindrical plot was very powerful, as you could sit outside it to see all the data, or sit in the middle and rotate around of slide up and down (both easier to ontrol than flying or lateral movements) to see more detail. The vertical dimension is used to show the different IP addresses being looked up.

The Detail

The obvious groups of 5 vertical bands represent Monday to Friday activity. What is immediately interesting is the amount of out-of hours activity (e.g #6). Some of this show near regularity (e.g. #4), but actually not regaulr enough to be picked up by a reliable script. There are also cases where an address gets near continuous calls (eg #1 and #2) and other cases where a vertically stacked set of calls indicate a single web page request triggering a whole host of DNS requests – as different images, ads and trackers are triggered (#3).

Datascape is a product of Daden Limited.

www.datascapevr.com info@datascapevr.com 0121 250 5678