### Description

At the 2020 brainstorm it was suggested that the DCERPC logging would support a higher level logging, as both dcerpc and smb can be very verbose. Zeek was mentioned as an example to look at. Concern was that it might hide evasion attempts.

A good start would be to get some examples.

### Related issues:

- Related to Task #4097: Suricon 2020 brainstorm
- Related to Feature #5413: DCERPC logging is not easy to use in analysis

### History

**#1 - 11/23/2020 01:14 PM - Victor Julien**

- Related to Task #4097: Suricon 2020 brainstorm added

**#2 - 06/29/2022 07:55 AM - Victor Julien**

- Related to Feature #5413: DCERPC logging is not easy to use in analysis added