Data Pillar Deliverables

1. Engineering solutions for Data pillar with a ZT lens:

   How can in use be secured? What are the different methods to secure data in use? It is important to remember data is use is the data that is in RAM and in use by applications. Typical solutions include data masking, encryption, truncation. However if a data is masked / encrypted / truncated in RAM, will an application be able to use the data for processing?

   How can data at rest be secured? What are the different methods to secure data at rest? Typical solutions include data masking, encryption, truncation. What about data persisted in notepads or wordpads? These files are typically produced as intermediary artefacts while processing data. The files themselves may not be persisted for long. But need to be secured while they are present on an asset for however short time frame that may be.

   Controls for data at rest are applied to files (TDE), databases (field level encryption), volumes (EBS). Deciding the most appropriate solution to a given situation.

2. Identification of protect surface:

   What is a protect surface from ZT perspective? How can a protect surface be identified? What is not a protect surface? Why is data central to protect surface? We have identified a protect surface, now what? How do organisations proceed from identification of protect surface to implementing controls to achieve ZT?

3. Data loss prevention using SQL proxy (to be developed)

4. Use cases for legacy solutions

   Presence of legacy solutions is nothing new across industries. How can ZT be implemented across legacy solutions? Especially in environments where Windows workgroups are in use and resources are not on any domain. Or an environment that has only *NIX systems? Legacy systems that contain sensitive data.

5. private cloud versus public cloud:

   With public clouds sharing the same space and market share as private clouds (/ on-premise environments), how is ZT implementation different in both the clouds and is it any similar?

6. risk based solutions (to be developed)