Knowledge Transfer - File Fingerprint Migration, MD5 to SHA3-256

Background

MD5 is largely seen as an insecure hash algorithm because a hash collision can be engineered relatively easily. The motivation to shift file fingerprint from MD5 to SHA3-256 is because the optics of using MD5 in any part of Kiteworks is not good and not because of an exploitable vulnerability. File fingerprint is exposed to end user via mail attachments in Web UI an is thus the most visible part of Kiteworks that still uses MD5 hence having higher priority in migration.