Below are the integration steps and the pre-requisites:
Pre-Req:
1. A user with a password available in Cyberark. The User must be available at the database level too. e.g. if a Sql Server Login user is - SqlAdmin. Then the Cyberark password vault should store the username as SqlAdmin and the password can be based on Citi's standard.
2. The certificate files are downloaded from the Cyberark server to the TDM's Fast Data Masker server. For my case I downloaded below files:
1. Client_1_28.crt
2. Client_1_28.p12
3. RootCA.crt

Integration Guide:

The URL which provides the password for the Vault user:
https://services-uscentral.skytap.com:10885/AIMWebService/api/Accounts?appid=<UserName>&safe=Test&object=testobject

Steps:
1. Import the certificate files to Chrome certificates to validate if the API is working properly.
2. Import the certificate files to <Fast Data Masker's Installation Path>/jre/lib/security/cacerts. The root and client certificates need to be imported. Keytool command is used to import the certificates:
keytool -importcert -file certificate.cer -keystore cacerts -alias "Alias"
Please make sure that the <Fast Data Masker's Installation Path>/jre/bin/java and keytool commands are used.
3. Copy the fatjar(Cyberark Plugin Extn) provided by Broadcom to <Fast Data Masker's Installation Path>/extensions and client_1_28.p12 file at <Fast Data Masker's Installation Path>/
4. Run the GTMAPPER.exe(FDM) and provide the server details and only provide the username in the following format:
ext:cyberark:<SQL UserName>
Please don't add any other characters as this is how the Fat jar is built. Documentation for the same is added below

https://techdocs.broadcom.com/us/en/ca-enterprise-software/devops/test-data-management/4-10/reference/Security-Plugins.html

P.S.: The server URL and Ports are hardcoded till the certification is complete. Once done I will put the same in a property file that can be used for other variables.

FDM's version is - 4.10.83.0 but it will work on any version >4.9.