I am providing my insights and please feel free to share your thoughts if i am deviating the discussion.

I believe the use case of the consumer account is "Consumer tries to access the S3 bucket in the producer account to run the queries against that using Athena in the consumer account". In this case when a bucket location is registered in data lake location in the producer side and all the access shared to consumer using lakeformation account (either LF tag or data catalog name we can restrict their access - Assumed producer has the db-table metadata in glue). I.e they can have access to model refined data. So, the consumer is able to access only the access given model refined data.

**Producer Account Steps:**

1. **Set Up KMS Encryption:** Ensure that the S3 bucket where your data resides is encrypted using AWS KMS encryption.
2. **Create Glue Crawler:** Create a Glue Crawler in the producer account to discover and catalog the data in your encrypted S3 bucket. Configure the crawler to use the appropriate data classification and schema settings.
3. **Run Glue Crawler:** Run the Glue Crawler to scan the encrypted S3 bucket, extract metadata, and create tables based on the discovered data.
4. **Configure Glue Data Catalog Permissions:** Make sure that the IAM role used by the Glue Crawler has the necessary permissions to access the KMS key used for encryption, as well as permissions to read the S3 objects.

**Lake Formation Setup:**

1. **Consumer Account:**
   * Create an IAM role in the consumer account that will be assumed by AWS Lake Formation to access the shared resources.
   * Attach a trust policy to the IAM role that allows AWS Lake Formation in the producer account to assume this role.
   * Configure KMS key permissions for the consumer IAM role, allowing it to use the KMS key associated with the encryption.
2. **Lake Formation Permissions:**
   * In the producer account, use Lake Formation to grant permissions to the IAM role in the consumer account for the Glue Data Catalog, the database, and the table created by the Glue Crawler.
   * Use the **--principal** parameter to specify the ARN of the consumer IAM role.
   * Grant the necessary permissions such as "SELECT," "DATA\_LOCATION\_ACCESS," and any other required permissions.
3. **Database and Table Sharing:**
   * Share the database and table from the Glue Data Catalog with the consumer account using the Lake Formation permissions.
   * The consumer IAM role will be able to access the data using the permissions granted through Lake Formation.

**Consumer Account Steps:**

1. **Data Querying:**
   * In the consumer account, use the consumer IAM role to query the shared database and table using tools like Amazon Athena.
   * AWS Lake Formation will handle the decryption of the data using the KMS key associated with the encryption.

By following these steps, you're allowing the consumer account to access and query the shared data from the producer's encrypted S3 bucket through AWS Lake Formation. The consumer IAM role's permissions, along with the Lake Formation configuration, ensure secure and controlled access to the data while transparently handling decryption using the appropriate KMS key.

Top of Form

I am providing my insights and please feel free to share your thoughts if i am deviating the discussion.

I believe the use case of the consumer is "Consumer tries to access the S3 bucket in the producer to run the queries against that using Athena in the consumer account". So When a bucket location is registered in data lake location in the producer side and all the access shared to consumer using lakeformation account (either LF tag or data catalog name we can restrict their access - Assumed producer has the db-table metadata in glue). I.e they can have acccess to particular model refined data. So the consumer able to access only the access given model refined data.