Data Protection Walkthrough

Tuesday, July 13, 2021

Attendees:

Kishore Puvvala

Machine generated alternative text:
O Oluwaseyi Mafi 
Host 
Jason Nazare 
O Aerozona Obiadazie 
LL Lisa Larsen 
O Moriah Striegel 
Olivia Lawson 
O Sol Vazquez 
O Tyrell Jarrett 

Location: WebEx

**AGENDA**

**Jason:** Overview on Data encryption for CDR. Who has access to change information? Walk us through how data is encrypted.

**Kishore Puvvala**: We check to see if there is any PII data to make sure its encrypted at rest. There are other levels of security we have. Data on disk in always encrypted. Data in transit should be secured. PII information through any tables is encrypted and secured. There are several security measures on EDP. With CDR, which is an operation use case. PII data is not encrypted (Exception) because its an operation level use case. Every other data is encrypted.

Every data we bring in, we use data injection ticket. Data team use the data dictionary to review this. They tag any column as PII column. Part of our ingestion process. The whole process, including targeting them, it's part of the JIRA ticket.

**Jason**: Is this information documented?

Yes. "Pretty Part" (Not sure on name) owns the process automation aspect. They document all these different types of ticket.

**Jason:** Do you have one of those Jira ticket to show us?

In the cloud, we are using Service now rather than JIRA.

Any data in CDR is through API, no SQL data analytics. When we pull the file into SQL, then we plan to implement data encryption tools. Also trying to decrypt data and query data and had over the consumer impacts our SLAs. So we do not bring encryption/decryption to any operational SLAs. We don't try to work with HTTPs, we only work HTTP. Every data is taken care of from the API gateway which is used for operation enterprise

The platform team has different operational groups. Who is managing the data security aspect (Platform Team). There are different teams supporting them. Disk level security, data level security. We are the owners. CVS is the owner. Handled by the platform team.

Two groups we walk with very close Cloud engineering, and Cloud security. We follow the security standards established by them. We hold the private keys, and the public key is what we share with Google.

In google, there are buckets (kind of like a file system) and also databases. They will be in the form of tables and columns. When we create new buckets and databases, the keys used are encryption cases. A database query mainly for CDR. Data sets and Data base, at these levels, we can apply encryption. For big query, we will apply column level security. (enterprise security team) - 3rd level security.