SOCCERTACT

YOUR IN-HOUSE DATA DEPARTMENT ON THE CLOUD

ESSENTIALS FOR A DATA DEPARTMENT

API INTEGRATION

AUTOMATED DATA PROCESSING AND ETL

DASHBOARDS

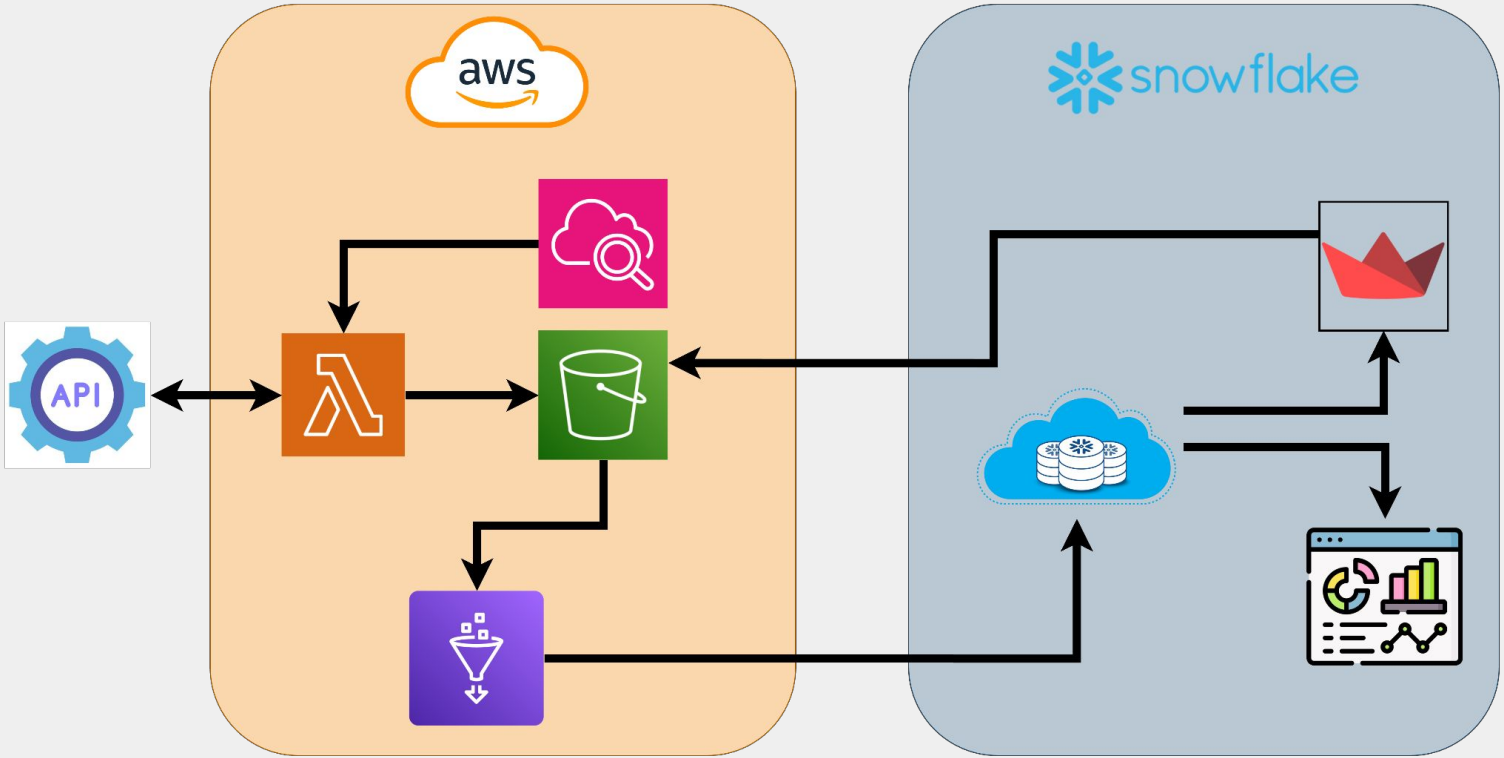
CENTRALIZED STORAGE

DOCUMENT UPLOAD

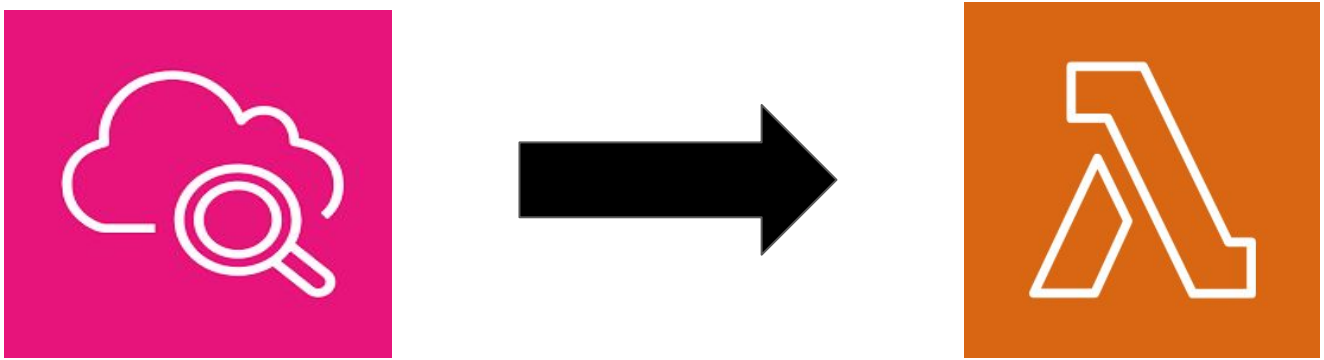
CROSS REFERENCE IDS

SECURITY

A CLOUD DATA DEPARTMENT



API INTEGRATION



To retrieve data from APIs on a schedule, Soccertact uses Amazon CloudWatch to set up a rule that triggers an AWS Lambda function at specified intervals (e.g., every day). The Lambda function then executes the API call, processes the response, and stores the data in a target location like Amazon S3 or a database. CloudWatch logs can be used to monitor the Lambda execution, track errors, and review successful data retrievals

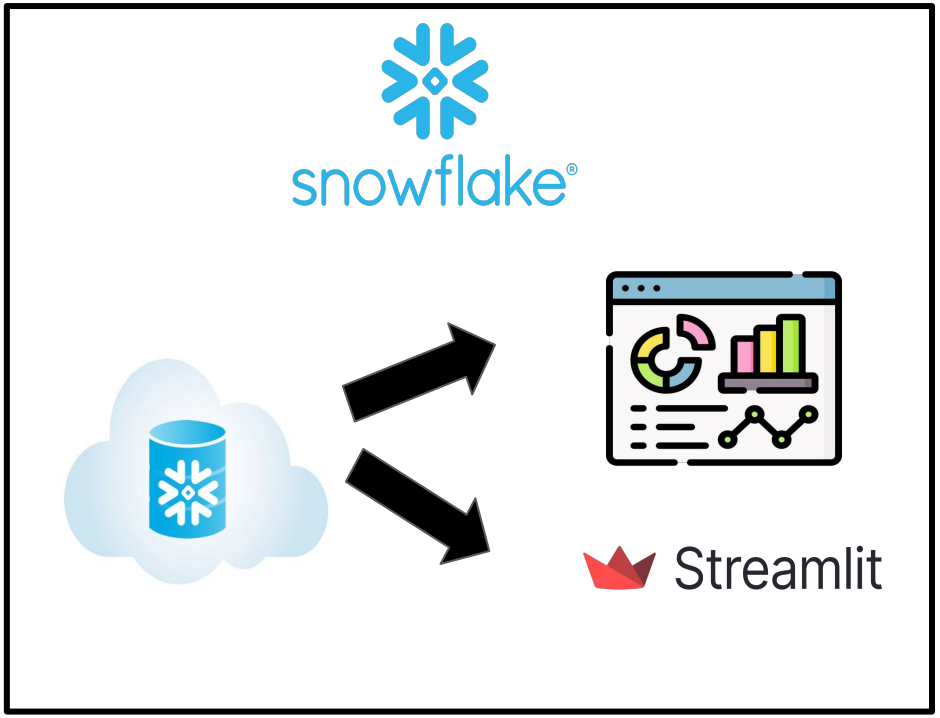
CENTRAL STORAGE

Soccertact uses Amazon S3 to store data from APIs or user-uploaded documents. This is achieved by allowing a Lambda function or front-end app to upload files directly to organized, secure buckets. This creates a centralized, encrypted storage for easy access and processing.

AUTOMATED DATA PROCESSING OR ETL

AWS Glue is a fully managed ETL service that can clean, transform, and prepare data from various sources for analysis. It can be used to process data retrieved from APIs or uploaded documents in S3 by defining ETL jobs that clean and structure the data. The transformed data is then stored in snowflake DB, making it ready for analysis.

UI & DASHBOARD



Soccertact uses snowflake which serves as a database for storage and easy access across the platform. Using Snowflake dashboards, users can visualize key insights directly within the Snowflake environment, while Streamlit as a UI layer offers an interactive, customized interface for users to explore the data. This integration supports seamless data management, real-time analytics, and an intuitive experience for end-users

DOCUMENT UPLOAD AND MANAGEMENT

Streamlit

With Streamlit, users can easily upload files, such as medical records or contracts, through a simple upload button. These files are then automatically stored in Amazon S3, keeping them secure and organized for easy access when needed. This process is smooth, ensuring important documents are managed effortlessly

SECURITY

In Snowflake, data is encrypted by default, and access can be controlled through strict user roles and permissions, ensuring only authorized people can view or edit sensitive information. Snowflake also offers data masking to protect private details, along with audit logs to monitor data access and activities.

In AWS, data is protected through encryption and user access controls, with tools like Identity and Access Management (IAM) to manage who can access different resources. AWS services are secured within a virtual network, and activity tracking is enabled through logging, allowing you to monitor actions and ensure data integrity.