Predictive – Case Study

Introduction

Predictive analytics is a set of business intelligence (BI) technologies allows it's users to uncover relationships and patterns within large volumes of data that can be leveraged to predict behavior and events. Unlike other BI technologies & approaches, predictive analytics is forward-looking, using past events to anticipate the future.

In the case of Incident Management, predicting IT Incident Resolution Time involves using incident data from an ITSM system to build a predictive model that can estimate the time it will take to resolve an incident based on its characteristics. The model can help IT teams better manage their incident workload and improve service level agreements (SLAs) by identifying incidents that are likely to exceed their resolution time targets.

Problem Statement

Your team is tasked to use incident data from an IT service management (ITSM) system to predict the resolution time of IT incidents. The dataset contains information about IT incidents, including the type of incident, the priority level, the time the incident was reported, and the time it was resolved.

We will use this dataset to build a predictive model that can estimate the time it will take to resolve an incident based on its characteristics. The model can help IT teams better manage their incident workload and improve service level agreements (SLAs) by identifying incidents that are likely to exceed their resolution time targets.

Additionally, the model can help identify bottlenecks in the incident resolution process, such as overloaded technicians or inefficient processes, which can be addressed to improve incident response times.

Additional Specifications

- Predictive Analytics to be accomplished using Snowflake.
- Use Stage and Load the Dataset in the Snowflake.
- Use snowflake table as input to the python rather than directly using the csv file.

Expected Outcomes

- Individual presentation file (Please use the PowerPoint template provided in Lumen). This needs to be uploaded to Lumen under the case study submission placeholder.
- Demonstration of the solution at the time of evaluation & viva.

Suggested steps to follow for this case study

1. **Data Collection**: Collect incident data from ITSM system, which includes information about the type of incident, the priority level, the time the incident was reported, and the time it was resolved. This step is completed – We have provided the Dataset.

2. **Data Preparation**: Prepare the data for analysis by cleaning and organizing it. This may include removing duplicates, handling missing data, and transforming data into a suitable format for analysis.

3. **Data Exploration**: Explore the data to identify patterns and relationships between different incident factors. Use data visualization tools and techniques to help identify these patterns.

4. **Feature Engineering**: Identify and extract features from the incident data that are relevant to predicting resolution time. This may include features such as incident type, priority level, user or system affected, and any other relevant data.

5. **Model Development**: Build a predictive model using machine learning techniques that can estimate the time it will take to resolve an incident based on its characteristics. This may involve training and testing different models to identify the best performing model.

6. **Model Validation**: Validate the predictive model using a hold-out dataset or cross-validation techniques to ensure it is accurate and reliable.

7. **Model Deployment**: Deploy the predictive model into a production environment, such as an ITSM system, to support incident resolution time prediction. This step is for future use – Not for Use Case

Understanding the dataset provided for the case study

The dataset for this use case contains incident data from an ITSM system. It includes information about the type of incident, the priority level, the time the incident was reported, and the time it was resolved. The dataset should also include additional columns that may be relevant to predicting resolution time, such as:

- **Incident Type**: The type of incident, such as hardware failure, software issue, or network outage. You need to find – depends on the prediction, but not mandate.

- **Priority Level**: The priority level assigned to the incident, such as high, medium, or low.

- **User or System Affected**: The user or system affected by the incident. You need to find – depends on the prediction, but not mandate.

- **Service or System Impacted**: The service or system impacted by the incident. You need to find – depends on the prediction, but not mandate.

- **Resolution Steps**: The steps taken to resolve the incident, including any delays or issues encountered. You need to find – depends on the prediction, but not mandate.

- **Incident Status**: The current status of the incident, such as open or closed.

- **Incident Age**: The time elapsed since the incident was reported.

- **Incident Volume**: The number of incidents reported over a given time.