AI\ML Enabled IT Operations

Introduction:

Enterprise systems span across on-prem and cloud with out any data logging standards to analyze data patterns related to IT incidents. AI/ML enabled IT Operations addresses this HUGE issue leveraging Machine Learning algorithms to predict hidden behavioral patterns in the vast amount of log file dataset (across all the platforms, e.g., Snowflake in AWS, Oracle data on-prem, etc.).

AI enabled IT operations detect the abnormal (anomalous) system behavior before it impacts services.

Challenges

1. Data source (columns) identification and data cleansing (remove data duplication, private data, etc.,).
2. Hidden data patterns analysis - identifying respective learning algorithm (Supervised or Unsupervised learning based on limited incident type data availability in the datasets.
3. Identify the algorithms for incident type categorization (*i.e., Cloud Maintenance Incident, Network Incident, Capacity Incident, User Service Request Incident etc.*)
4. Figuring out which AI model to use (based on Accuracy, Precision or F1 score, etc.), performance of model is calculated using 5-fold cross validation.
5. Further analysis of hidden patterns to narrow down on incident sub-categorization of incidents based into other dimensions like incident time, process impacted, services impacted.
6. Based on sub categorization map these incidents against actual business impacts.
7. Determine the return on investment against categorized impacted incident.

List of challenges:

Dynamic IT environment: The IT environments can automatically scale up or down using technologies like orchestration of containers as per the demand. Manual analysis of such environment is really challenging.

Increased Monitoring Complexities: Automation has introduced many new components in IT infrastructure architecture. These new components also need to be monitored along with other regular metrics such as CPU utilization, network, memory, application logs etc.

IT service outage or latency issues: Businesses get affected by IT failure or service outage or latency issue. This might cost significantly, which leads to low productivity. Therefore, IT operations must be proactive and efficient, such that when an issue arises it can be solved promptly.

High Volume of ITSM Tickets & Less Expert Staff: IT teams have a hard time handling the large amount of tickets with less expert support staff leading to delayed resolution and deployments.

Data in silos & Volume: A typical IT infrastructure produces a large amount of data in form of metrics, ITSM tickets, logs, traces, and alerts. This data is present in silos and challenging to monitor.

Multiple monitoring tools & platforms.

No data logging standard

Solution:

Process Flow steps list here.

- UCI machine Learning repository and various inferential (its real time data) data sources are used for model building & training.
- Blend of different libraries such as (*regex, Stanford NLP, NLTK, pandas, Scikit-learn, matplotlib, seaborn, joblib*) were used for cleansing and removal of PII (Personal Identifiable Information) data.
- Unsupervised machine learning approach was applied based on dataset analyzed to fetch hidden patterns of (incident types) residing within descriptive fields.
- Applied commonly used algorithms to converting the textual data to numerical vector formats. The countvectorizer is used for this. This would help in model training & prediction.
- 5-fold cross validation training-testing was applied to determine the best model considered for this use case.
- Further sub-categorization was applied using same techniques.
- The sub-categorization is used to predict the resolution time, impact of environmental change, and change request failure.
- Insightful actionable dashboards are presented for taking business decisions.

AI enabled IT operation is the solution to above challenges.

Some features of AI enabled IT operations system are listed below:

Anomaly Detection: Anomaly detection works on outlier detection algorithms. It tracks a single KPI by comparing its present and historical behavior. If the score becomes high, it can create an alert.

Root Cause Analysis: RCA helps to identify potential root cause of incident faster and reach the solution in less time. This helps the business to improve MTTR and save man hours.

Predictive Analytics:

- Automatic ticket categorization into appropriate incident categories helps in the faster and more accurate allocation of tickets to correct assignment groups.
- Prediction of resolution time of ticket will help to prioritize the ticket for resolution.
- Predicting the possible incidents on change request or environment change, helps to fix the probable issues faster before it becomes a system wide incident.

Benefits:

- Auto self-healing of incidents
- Improve the customer satisfaction by minimizing downtime
- Creating more actionable insights from siloed data
- Cost saving because of man hour savings on Root cause analysis
- Faster mean time to resolution (MTTR)
- Reduced operational cost
- From reactive to proactive approach in incident management