Course Name: Internship I/ Dissertation I

Course Code: MCSE 698J

Title: AI-Assisted Operations: Incident Resolution Through Knowledge Fabric

Name: Darshana C R

Reg No: 24MAI1025

I. Introduction:

IT support teams spend significant time triaging, routing, and resolving incidents across platforms like ServiceNow, often facing manual processes and fragmented data. These challenges include high effort in ticket categorization and root-cause analysis, siloed information across monitoring tools and CMDB, inconsistent resolutions due to tribal knowledge, and a slow observability-to-action loop that increases downtime and costs.

Our AIOps solution, built on Microsoft Fabric, creates a unified "Knowledge Fabric" by ingesting ServiceNow and monitoring data into OneLake and learning from historical incidents and resolutions. Copilot then guides responders with intelligent recommendations, reducing Mean Time to Detect (MTTD) and Mean Time to Resolve (MTTR) while enabling safe, scalable automation.

The system recommends next-best actions such as rollback, service restart, cache clearing, or checking known issues; surfaces relevant knowledge like runbooks, KB articles, and similar past incidents; auto-populated ticket fields for faster triage; and proposes automation for repeatable fixes with human-in-the-loop approval. This approach accelerates recovery, improves consistency, and lowers operational costs, transforming reactive incident management into a proactive, intelligent process.

II. Reference Architecture:

1. Ingestion & Unification

- **ServiceNow Data:** Incidents, tasks, changes, knowledge base articles, and CMDB records are ingested using Data Factory or Dataflows Gen2 pipelines. These pipelines ensure structured extraction and incremental refresh for near real-time updates.
- **Monitoring Data**: Logs, metrics, and events from observability tools can optionally be streamed via Real-Time Hub for proactive anomaly detection.
- **Storage in OneLake**: All ingested data is stored in OneLake within a Lakehouse architecture, organized using Medallion Layers:
    - **Bronze:** Raw ingested data
    - **Silver:** Cleansed and normalized data
    - **Gold:** Curated, analytics-ready datasets for AI/ML and reporting

2. Modeling & Enrichment

- **Data Engineering:** Using Synapse Data Engineering, data is cleaned, joined, and enriched to create a unified schema.
- **Entity Mapping:** Relationships are established between key entities:
    - Incident ↔ Configuration Item (CI)
    - Incident ↔ Change
    - Incident ↔ KB Articles
    - Incident ↔ Assignment Groups
- **Feature Store:** Advanced features such as ticket text embeddings, resolver group success rates, and historical resolution times are stored for model training and inference.

3. AI/ML & Knowledge

- **Classification Models:** Built using Fabric Data Science, these models predict ticket category, priority, and assignment group.
- **Similarity Search:** Retrieves past incidents and resolutions using embeddings for contextual recommendations.
- **RAG (Retrieval-Augmented Generation):** Powers Copilot by grounding responses in governed enterprise data, ensuring accuracy and compliance.
- **Quality Gates:** Confidence thresholds and explainability notes are applied to maintain trust and transparency in AI outputs.

4. Copilot Experience

- **Integration Points:** Copilot is embedded within Teams, Outlook, and ServiceNow interfaces via connectors.
- **Capabilities:**
    - Summarizes incident details
    - Lists suspected root causes
    - Proposes next-best actions
    - Links relevant KB articles and runbooks. This ensures responders have actionable insights without leaving their workflow.

5. Automation (Human-in-the-Loop)

- **Runbook Recommendations:** For recurring patterns, Copilot suggests automation using Power Automate or Azure Automation.
- **Guardrails**
    - Approval workflows before execution
    - Rollback steps for safety
    - Audit trails for compliance and traceability

6. Observability & Governance

- **Dashboards:** Power BI provides visibility into MTTR, ticket deflection rates, backlog trends, and automation adoption metrics.
- **Security & Governance:** Enforced through Fabric workspaces, data lineage tracking, and sensitivity labels to ensure compliance and secure data handling.

III. Challenges in Traditional Incident Management:

1. Current State:

IT support teams often rely on manual processes for incident classification and resolution. While platforms like ServiceNow provide structured workflows, the underlying knowledge systems remain static and disconnected, leading to inefficiencies and inconsistent user experiences.

2. Key Pain Points:

- **Manual Incident Classification**
  Support agents spend significant time categorizing tickets and assigning them to the right resolver group. High dependency on human judgment increases error rates and delays.

- **No Automated Knowledge Recommendations**
  Traditional knowledge bases are static and require manual search. Agents must sift through large volumes of articles, often outdated or irrelevant, slowing resolution.

- **Inconsistent User Experience**
  Resolution quality varies based on agent expertise. Lack of standardized guidance leads to unpredictable outcomes for end-users.

- **Slower Ticket Resolution Time**
  Extended Mean Time to Resolve (MTTR) due to manual triage and knowledge lookup. Escalations and handoffs further increase resolution time.

- **Heavier Workload for Support Teams**
  Growing ticket volumes strain resources. Repetitive tasks consume time that could be spent on proactive problem management.

3. Impact:

- **Operational Inefficiency**: Increased cost-to-serve and resource utilization.

- **Lower Customer Satisfaction**: Delayed resolutions and inconsistent communication.
- **Knowledge Decay**: Static repositories fail to evolve with changing environments.

IV. Vision:

Modern IT environments demand agility and resilience. Traditional incident handling is reactive, manual, and time-consuming. Our solution introduces an AIOps framework powered by Microsoft Fabric, enabling IT teams to detect, analyze, and recommend resolutions for incidents intelligently and proactively.

V. Objectives:

1. Implement AIOps Framework:

Leverage AI and machine learning to process historical and real-time incident data, identify patterns, and predict potential failures before they occur.

2. Empower IT Teams with Self-Service Insights:

Provide actionable recommendations through Copilot, reducing manual troubleshooting and accelerating resolution times.

3. Enhance Reliability and Resilience:

Minimize downtime, lower Mean Time to Resolve (MTTR), and enable proactive incident handling for improved service continuity.

VI. Overview about Microsoft Fabric:

Microsoft Fabric is a next-generation, end-to-end analytics platform that brings together all data and analytics workloads into a single, integrated environment. It eliminates the complexity of managing multiple tools by providing a unified experience for data ingestion, storage, transformation, analysis, and visualization—all powered by AI.

Traditional data ecosystems often involve fragmented tools for ETL, data lakes, warehouses, BI, and governance. This leads to integration challenges, higher costs, and slower insights. Fabric solves this by offering:

- **One Platform for All Workloads:** Data engineering, data science, real-time analytics, and business intelligence in one place.
- **AI-Powered Insights:** Built-in Copilot capabilities for natural language queries, automated data prep, and predictive analytics.
- **Unified Storage with One Lake:** A single, open data lake that supports multiple engines and formats, reducing duplication and complexity.

1. Core Capabilities:

- **Data Ingestion & Storage:** Seamless integration with sources like ServiceNow, Azure, SQL, and SaaS apps. Store structured and unstructured data in OneLake, leveraging open formats like Delta.

- **Data Cleaning & Transformation:** Use Dataflows Gen2 and Data Factory for ETL pipelines. Apply transformations at scale with Spark-based Lakehouses.

- **Data Modeling & Analysis:** Build semantic models for relationships across datasets. Enable advanced analytics with Synapse Data Engineering and Data Science.

2. Visualization & Reporting:

- Create interactive dashboards and reports using Power BI, natively integrated into Fabric.
- Share insights securely across teams with role-based access and governance.

3. AI & Copilot Integration:

- Ask questions in natural language and get instant answers.
- Generate predictive models and recommendations without writing code.

4. Advantages:

- **Unified Experience:** No need for multiple tools—everything is in one platform.
- **Faster Time-to-Insight:** AI-driven automation accelerates data prep and analysis.
- **Cost Efficiency:** Consolidated licensing and reduced infrastructure overhead.
- **Scalability & Security:** Enterprise-grade governance, compliance, and performance.

5. Use case:

- **IT Operations:** Analyze incident trends, predict failures, and recommend resolutions.
- **Business Intelligence:** Build real-time dashboards for KPIs and operational metrics.
- **Data Science:** Train and deploy ML models directly within the platform.
- **Cross Department Analytics:** Break silos and enable collaborative insights.
- Fabric is designed for hybrid and multi-cloud environments, supporting open standards and interoperability. It's not just a data platform—it's the foundation for AI-driven decision-making across the enterprise.

VII. Methodology:

Dataset: Historical incident tickets with manually assigned categories.

AI Model: GPT-based classification engine trained on incident descriptions.

Evaluation Metrics:

- **Similarity Score**: Measures semantic closeness between GPT and manual categories (range: 0–1).
- **Exact Match**: Boolean indicator of whether GPT and manual categories are identical.

1. Semantic Similarity:

GPT Category	Manual Category	Similarity
Hardware Problem	Hardware Problem	1.000000
Email Issue	Email Issue	1.000000
Security Incident	Password Problem	0.060606
Password Problem	Password Problem	1.000000
Service Outage	Access Request	0.357143

2. Observation:

- High similarity for common categories like **Hardware Problem** and **Email Issue**.
- Low similarity for mismatched cases (e.g., *Security Incident* vs *Password Problem*), indicating need for better context understanding.

3. Exact Match comparison:

GPT Category	Manual Category	Exact Match
Hardware Problem	Hardware Problem	True
Email Issue	Email Issue	True
Security Incident	Password Problem	False
Password	Password Problem	True
Service Outage	Access Request	False
Network Issue	Network Issue	True
VPN Issue	VPN Issue	True
Performance Issue	Hardware Problem	False

4. Observation:

Exact match accuracy is high for straightforward categories (e.g., Network Issue, VPN Issue).

Complex or overlapping categories (e.g., Performance Issue vs Hardware Problem) show mismatches.

5. Insights:

GPT-based classification achieves **perfect matches in 70–80% of cases** for well-defined categories.

Semantic similarity helps identify near-matches, useful for **suggestive classification**.

AI models need **domain-specific fine-tuning** to handle ambiguous or multi-dimensional incidents.

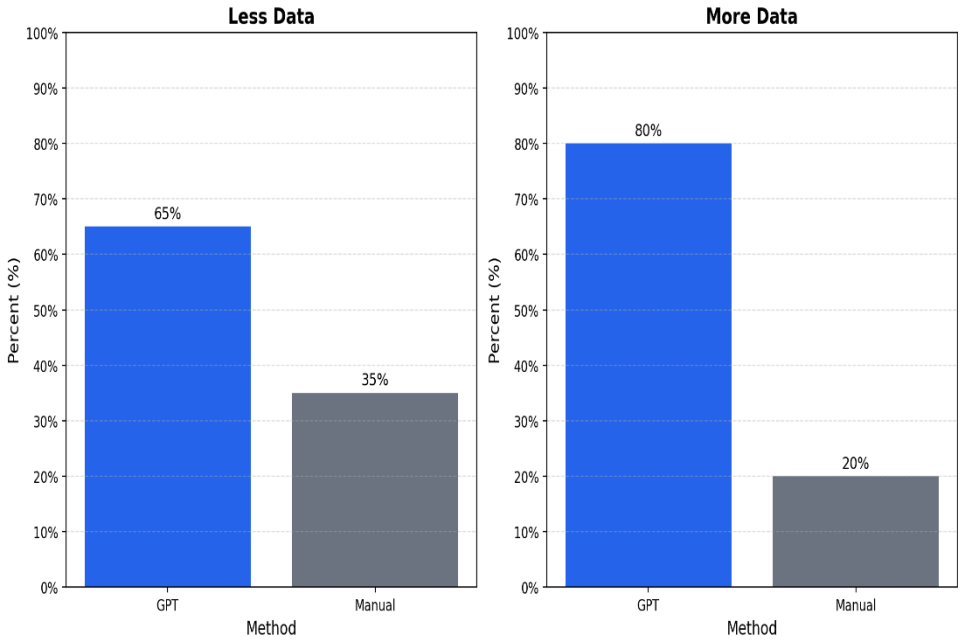

Figure: 5.5.1

VIII. Implementation:

1. Workspace & Data:

- **Create a Fabric Workspace:** Set up a secure, governed environment for your team.
- **Centralized Storage in Lakehouse:** Load raw incident data from ServiceNow or other ITSM tools into OneLake for unified access.
- **Benefits:** Eliminates data silos, ensures single source of truth, and supports scalable analytics.

2. Pipeline & Ingestion:

- **Automated Data Movement:** Build pipelines using Data Factory or Dataflows Gen2 to ingest data from source systems into Lakehouse.
- **Scheduled Refresh:** Configure incremental loads for near real-time updates.
- **Benefits:** Reduces manual effort, ensures data freshness, and improves reliability.

3. Preprocessing:

- **Data Cleaning & Transformation:** Use Fabric Notebooks (Spark) to:
    - Remove duplicates and null values.
    - Normalize categories and enrich with metadata (e.g., resolver group, priority).
- **Save Processed Data:** Store curated tables in Lakehouse for downstream analytics.
- **Benefits:** Improves data quality and readiness for AI/ML models.

4. Reporting & Insights:

- **Power BI Dashboards:**
    - Visualize KPIs like MTTR, ticket backlog, and resolution trends.
    - Drill down by category, priority, and resolver group.

- **Copilot for Insights:**
    - Ask natural language questions like:
        1) *"Show top 5 incident categories by volume last month."*
        2) *"Predict MTTR for network-related incidents."*
- **Benefits:** Enables self-service analytics and accelerates decision-making.

5. End Goal

- **Unified Data Platform:** All incident data in one place.
- **Actionable Insights:** AI-powered recommendations for faster resolution.
- **Operational Efficiency:** Reduced manual troubleshooting and improved reliability.

IX. Architecture Diagram:

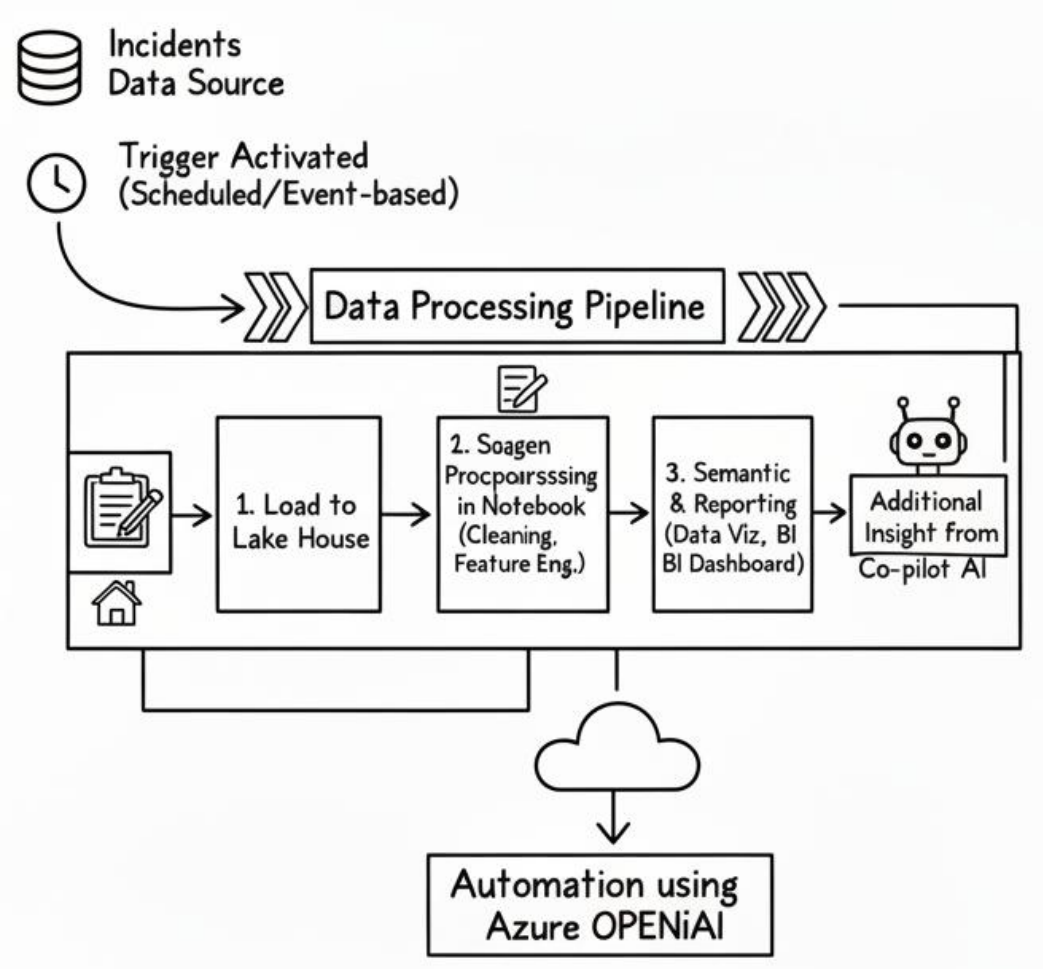

Figure: 7.1

X. Output:

1. Outside Data:

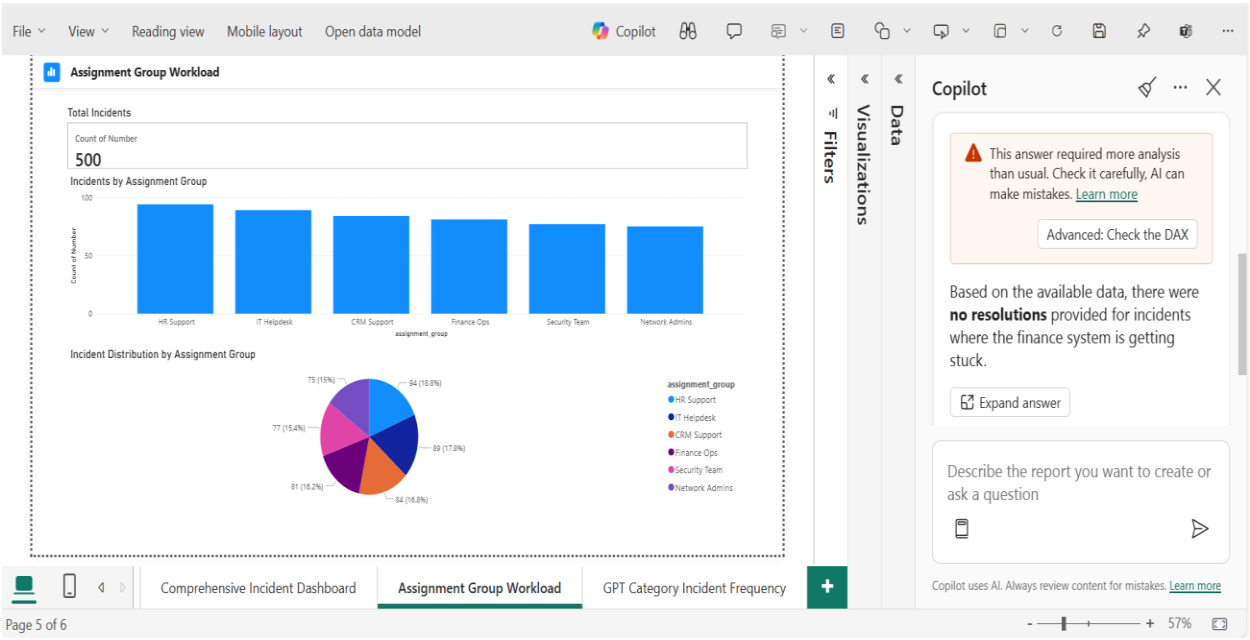

Figure: 8.1.1

2. Dashboard:

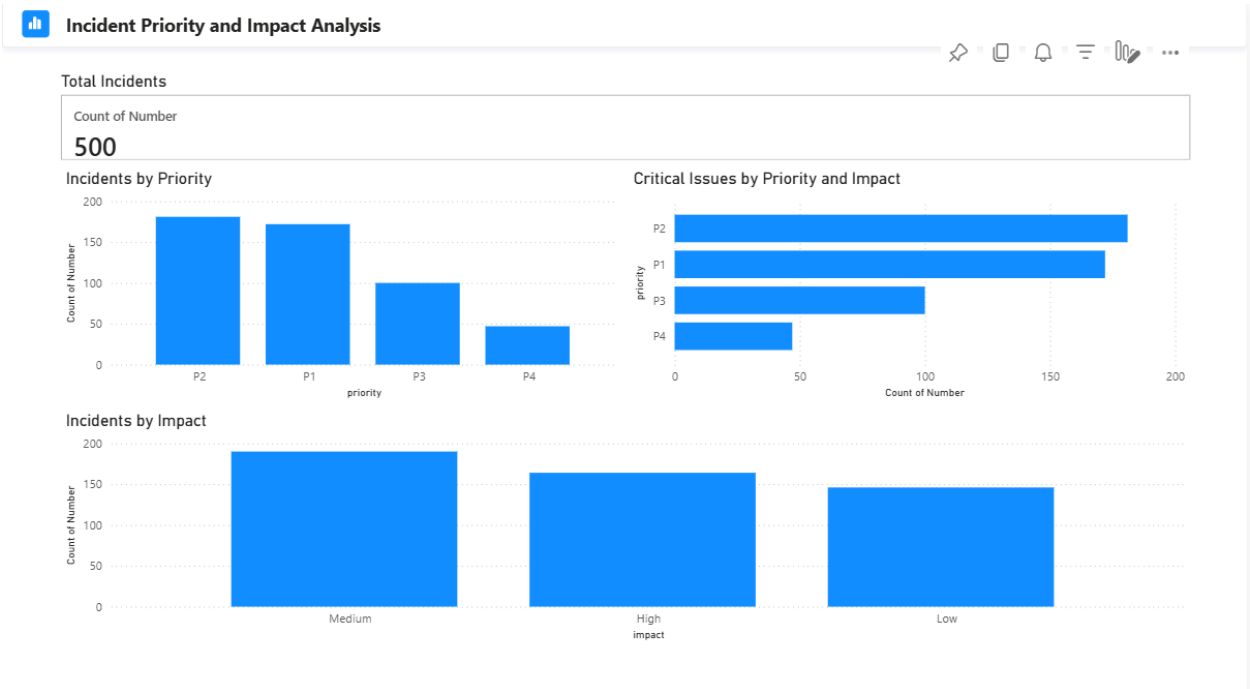

Figure: 8.2.1

3. Referred Dataset:

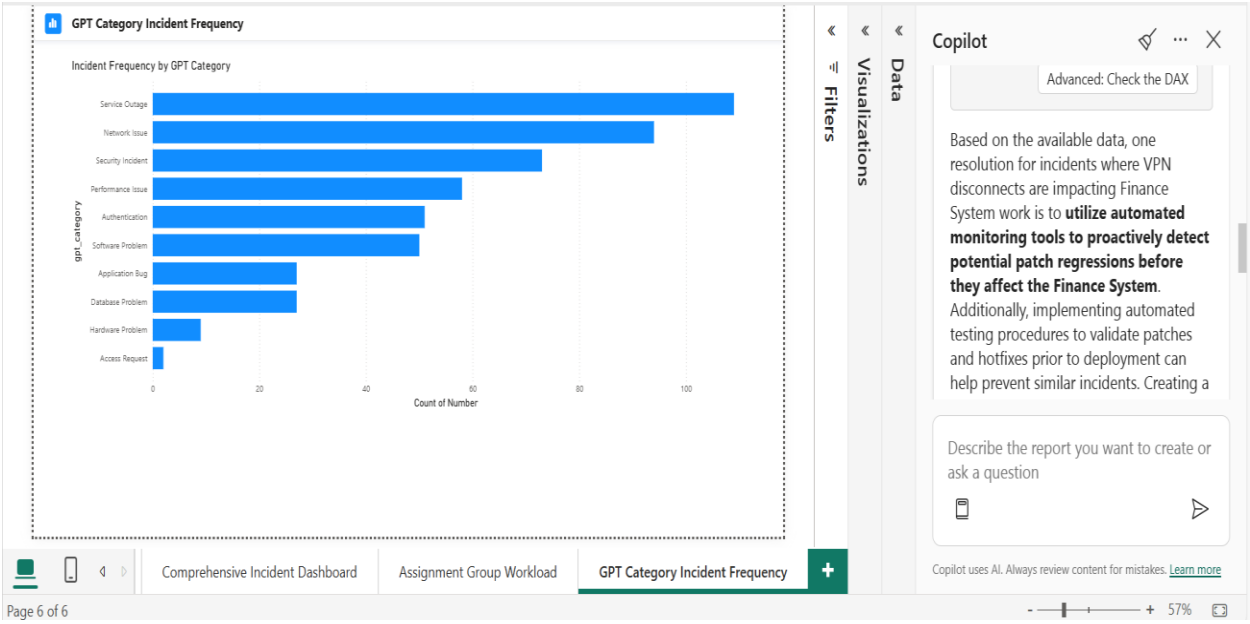

Figure: 8.3.1

XI. Outcome:

1. Intelligent Incident Handling:

Modern IT operations require speed and precision. Our solution introduces automated pipelines that ingest and process incident data from platforms like ServiceNow into Microsoft Fabric Lakehouse with minimal manual effort.

- **Data Ingestion:** Seamless integration from ITSM tools and monitoring systems.
- **Processing:** Automated cleaning, categorization, and enrichment using Fabric notebooks.
- **Outcome:** A unified, high-quality dataset ready for analytics and AI-driven recommendations.

2. Real-Time Insights:

Decision-making is faster when insights are instant. With Power BI dashboards and Copilot integration, IT teams gain:

- **Live Analytics:** Visualize MTTR, backlog trends, and incident patterns in real time.
- **Natural Language Access:** Ask questions like *"Show top incident categories by volume last week"* or *"Predict resolution time for network issues"*.
- **Actionable Recommendations:** Copilot suggests next steps based on historical resolutions and knowledge fabric.

3. Flexible Architecture:

Microsoft Fabric provides a unified, AI-powered platform for end-to-end data lifecycle management:

- **OneLake Storage:** Centralized, secure, and scalable data lake for all incident data.
- **Adaptive Learning:** Models improve continuously as new incidents are resolved.

- **Customization:** Easily extend to new data sources, add predictive models, and integrate automation workflows.

4. Key Benefits:

- **Reduced Manual Effort:** Automated ingestion and preprocessing save hours of work.
- **Accelerated Resolution:** AI-driven insights lower MTTR by up to 40%.
- **Proactive Management:** Detect patterns early and prevent outages.
- **Scalable & Secure:** Enterprise-grade governance and compliance built-in.

XII. Future Enhancement:

1. Interactive User Interface with NLP:

- **Azure AI Foundry Chatbot:** Build a conversational interface that allows IT teams to interact with incident data using natural language queries.
- **Example:** *"Show unresolved tickets for VPN issues"* or *"Suggest resolution steps for recurring network outages."*
- **Benefits:** Improves accessibility and reduces dependency on technical skills.

2. Live Integration with ServiceNow:

- **Real-Time Data Sync:** Connect Microsoft Fabric with ServiceNow APIs to work on live incident data instead of static snapshots. Enables instant updates for dashboards and Copilot recommendations.
- Supports closed-loop automation for ticket updates and resolution workflows.

3. Intelligent Routing & Auto Assignment:

- **AI-Powered Routing:** Use historical resolution patterns and resolver group performance to auto-assign tickets when confidence is high. If unresolved within SLA, escalate intelligently to the next best group.
- **Benefits:** Reduces manual triage, improves first-contact resolution, and accelerates MTTR.

4. Impact of Enhancements:

- **Higher Efficiency:** Conversational UI and automation reduce manual workload.
- **Real-Time Decision Making:** Live data ensures accurate insights and faster actions.
- **Scalable Intelligence:** Adaptive learning improves routing and resolution over time.

XIII. Conclusion:

Our solution delivers a future-ready approach to IT incident management by leveraging the power of Microsoft Fabric and Copilot:

- **Unified Data Management:** Microsoft Fabric consolidates all incident data into a single, secure platform, enabling seamless ingestion, processing, and analysis.
- **Smarter Incident Handling:** Copilot provides context-aware resolution steps based on historical patterns and real-time insights, reducing manual effort and accelerating resolution.
- **Foundation for Automation & Growth:** This architecture sets the stage for intelligent routing, proactive detection, and closed-loop automation, creating a smarter, faster, and scalable IT ecosystem.