SituationPlanet

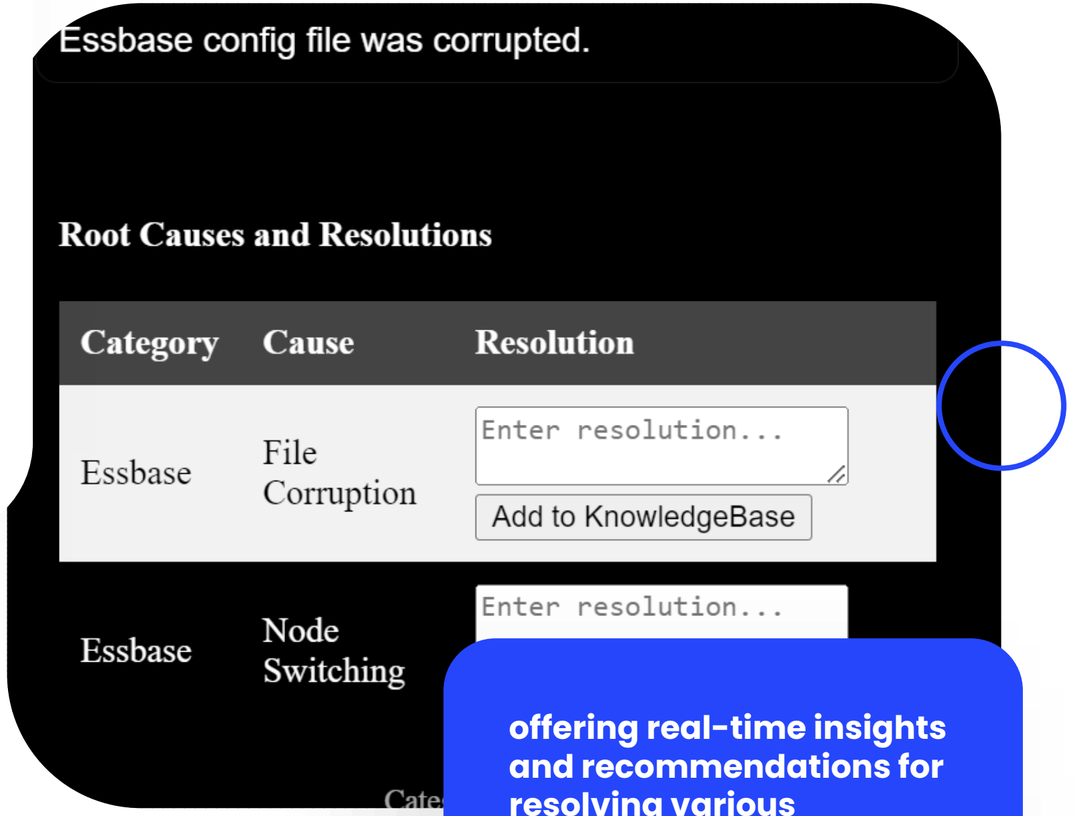
An AI Approach to Incident Management
by Aaditya Rengarajan (21Z202)

PSG Hackathon

ABOUT THE SOLUTION

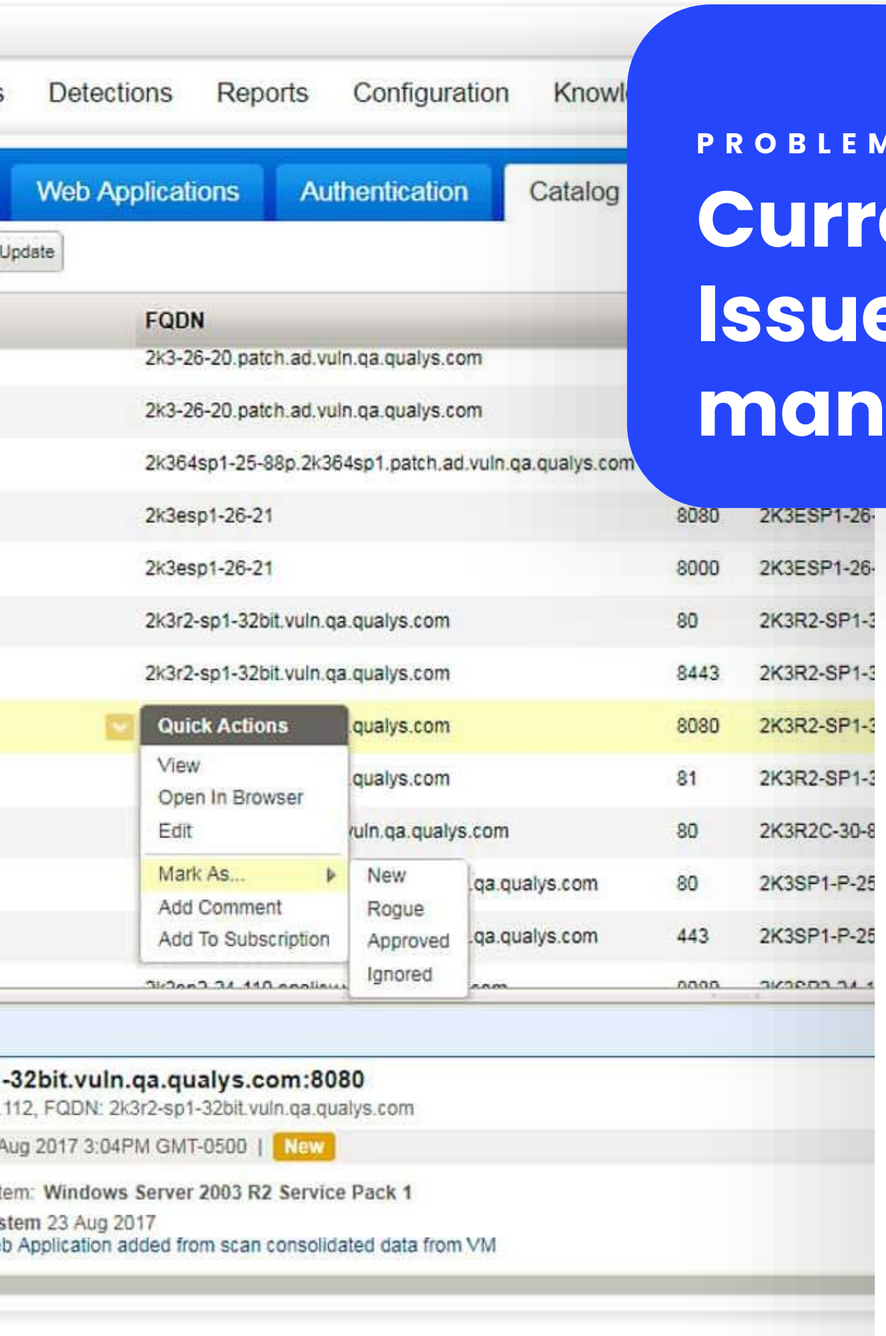
SituationPlanet Incident Assistant —

AI-powered incident management system that utilizes advanced natural language processing (NLP) and machine learning techniques to streamline the incident resolution process. It aims to provide a comprehensive solution for identifying incident categories, suggesting resolutions, and even implementing 'SelfHeal' technology to automate the incident resolution process.



offering real-time insights and recommendations for resolving various incidents.

An AI Approach
to incident management



PROBLEM STATEMENT

Current Issues with incident management processes

Situation
Planet

AI-Based Incident Management Approach

1. Manual and Reactive Processes

Traditional incident management often relies on manual monitoring and reaction. This approach can result in delays in identifying and addressing issues, leading to extended downtime and poor customer experiences.

2. Combinatorial Explosion

With a multitude of distinct incident types and their corresponding resolution techniques, manually exploring every combination is infeasible. By leveraging historical incident data and machine learning, SituationPlanet efficiently narrows down the immense array of options, enabling rapid and accurate resolution suggestions that significantly alleviate the burden of exhaustive manual exploration.

THE SOLUTION APPROACH

Solution Pipeline

01 Incident Classification

When a new incident is reported, the system analyses the incident description using Natural Language Processing (NLP) techniques. This categorizes the incident into predefined types, providing a clear understanding of the problem at hand.

02 Root Cause Analysis

The system delves into the details of the incident, including logs and historical data. Machine Learning algorithms identify underlying factors contributing to the incident, enabling efficient and accurate root cause identification.

03 Learn from History and Knowledge-Base

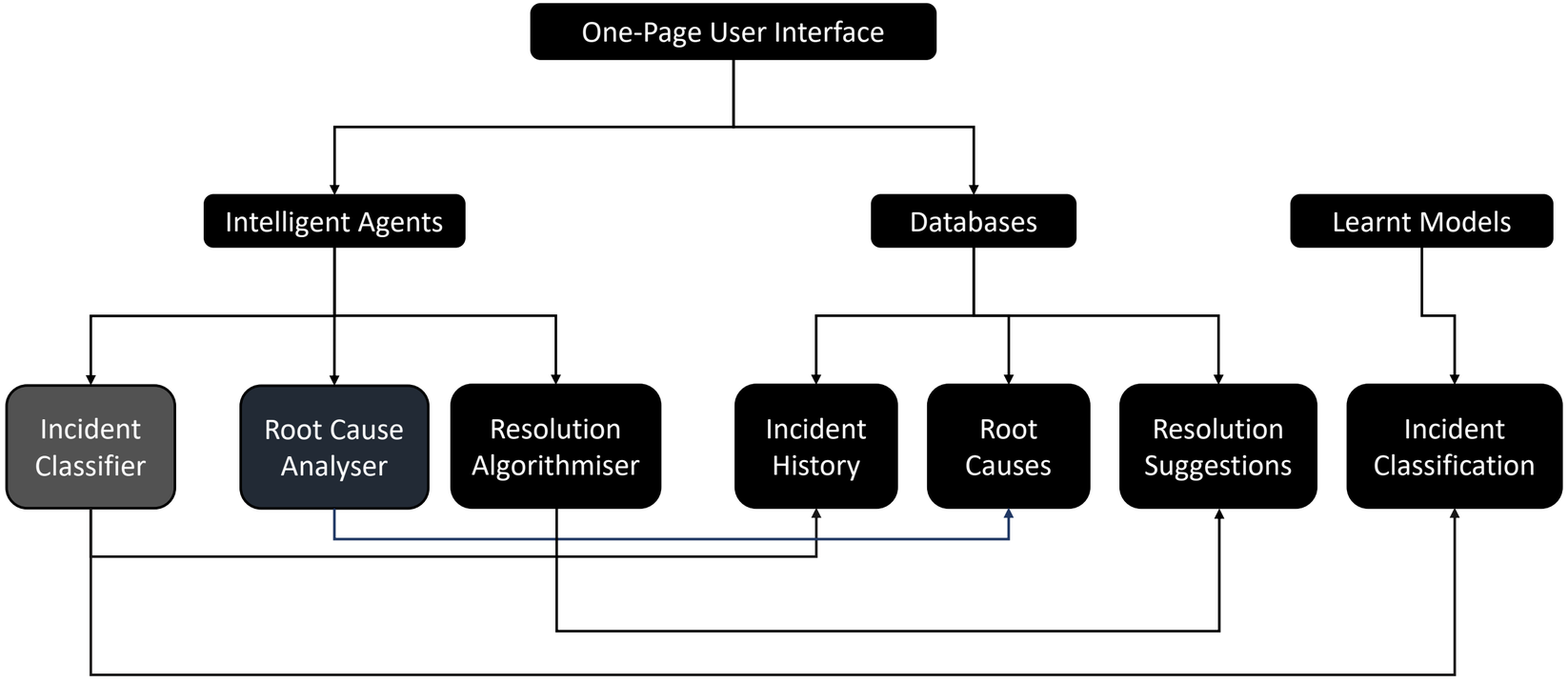
Leveraging historical incident data and a knowledge base, the system learns from the past. Machine Learning continuously evolves by integrating new incident data, enhancing its ability to make informed decisions.

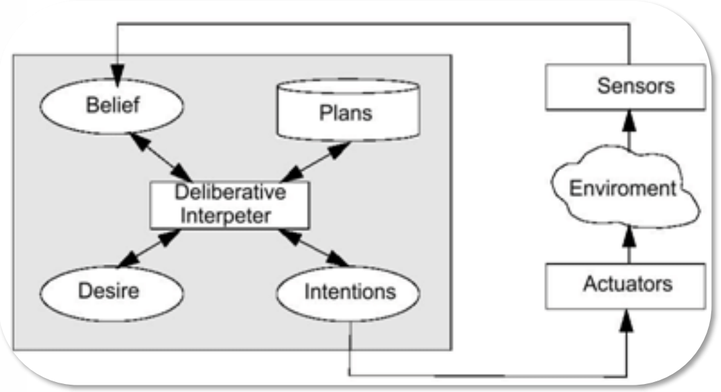
04 Propose Resolutions to specific root-causes

Armed with categorized incidents and their root causes, the system matches the incident's root cause to relevant resolution techniques. Drawing from the knowledge base, the system recommends a range of strategies tailored to address the specific issue's underlying causes.

SOLUTION OVERVIEW

Solution Structure and Posteriori Analysis

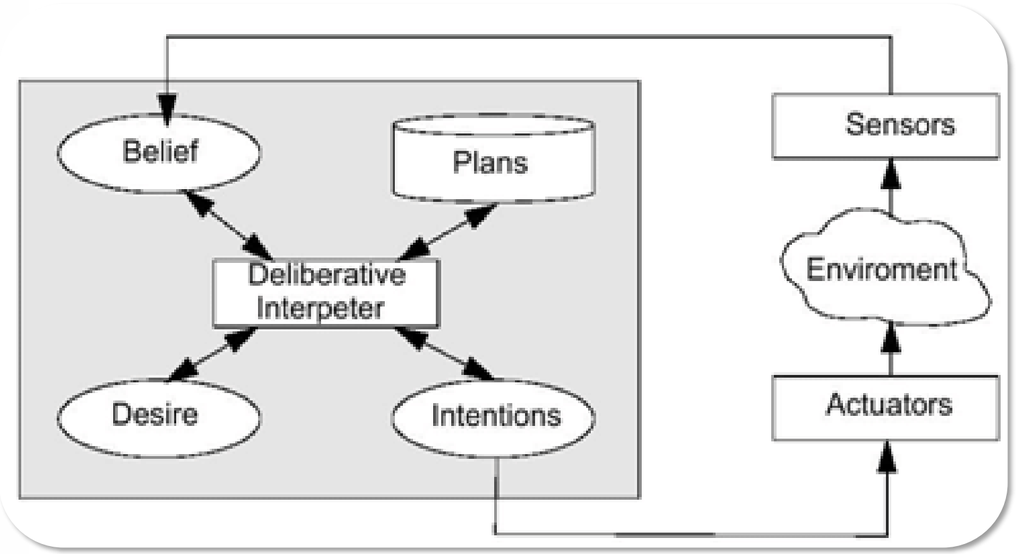




Situation
Planet

INTELLIGENT AGENT

Use of AI/ML as Deliberative Agent



How our Deliberative Agents leverage informed decision making, solving the problem of Combinatorial Explosion:

- Intelligent Decision-Making:
- Data-Driven Insights
- Resolution Recommendation
- Dynamic Learning
- Complex Decision Contexts
- Customized Suggestions

INTELLIGENT AGENTS

PEAS and Description of Intelligent Agents

01.

1. Incident Classifier

Performance Measure:
Accuracy of incident categorization, speed of classification.

Environment:
Incoming incident descriptions, historical incident data.

Sensors:
Incident descriptions, historical incident data.

Function:

- Analyzes incident descriptions using NLP techniques.
- Matches incidents to predefined categories.
- Provides accurate and quick incident categorization.

02.

2. Root Cause Analyser

Performance Measure:
Accuracy of root cause identification, speed of analysis.

Environment:
Incident data, system logs, historical incident data.

Sensors:
Incident data, system logs, historical incident data.

Function:

- Analyzes incident details and relevant logs.
- Identifies underlying causes of incidents.
- Helps prevent recurrence by addressing root issues.

03.

3. Resolution Algorithmiser

Performance Measure:
Effectiveness of resolution suggestions, relevance to incident.

Environment:
Incident data, resolution techniques knowledge base.

Sensors:
Incident data, resolution techniques knowledge base.

Function:

- Examines incident category and details.
- Matches incidents to appropriate resolution techniques.
- Offers a range of strategies for incident resolution.

SelfHeal WatchDog

SelfHeal WatchDog Technology

The system continuously monitors incoming incidents and uses its trained models to recognize patterns and similarities in incident descriptions. When it identifies an incident that closely matches a previously resolved issue, it triggers the 'SelfHeal WatchDog' process.

'SelfHeal' reduces the time required to resolve common and repetitive incidents by automating the remediation process.

```
if __name__ == "__main__":
    event_handler = LogFileHandler()
    observer = Observer()
    observer.schedule(event_handler, path=os.path.di
    observer.start()

    try:
        while True:
            time.sleep(1)
    except KeyboardInterrupt:
        observer.stop()
    observer.join()
```

[situationPlanet] WatchDog Alert! Inbox ×

21Z202 - AADITYA RENGARAJAN <21z202@psgtech.ac.in> 5:12 PM (0 minutes a

to me

Identified Log: `Failed FTR from upstream to downstream. KeyError.`

Log Category: **FTR**

Category	Cause	Resolution
FTR	Connection Issues	Check Network Connectivity Check Status of External Server Ping Test Internal, as well as External Server Ensure DNS Server Up-To-Date
FTR	API Miscommunication	Review API documentation and expected requests. Inspect request logs and responses for inconsistencies. Contact API provider for assistance if necessary.
FTR	File System Errors	Check permissions and ownership of affected directories. Create missing

SELF HEAL

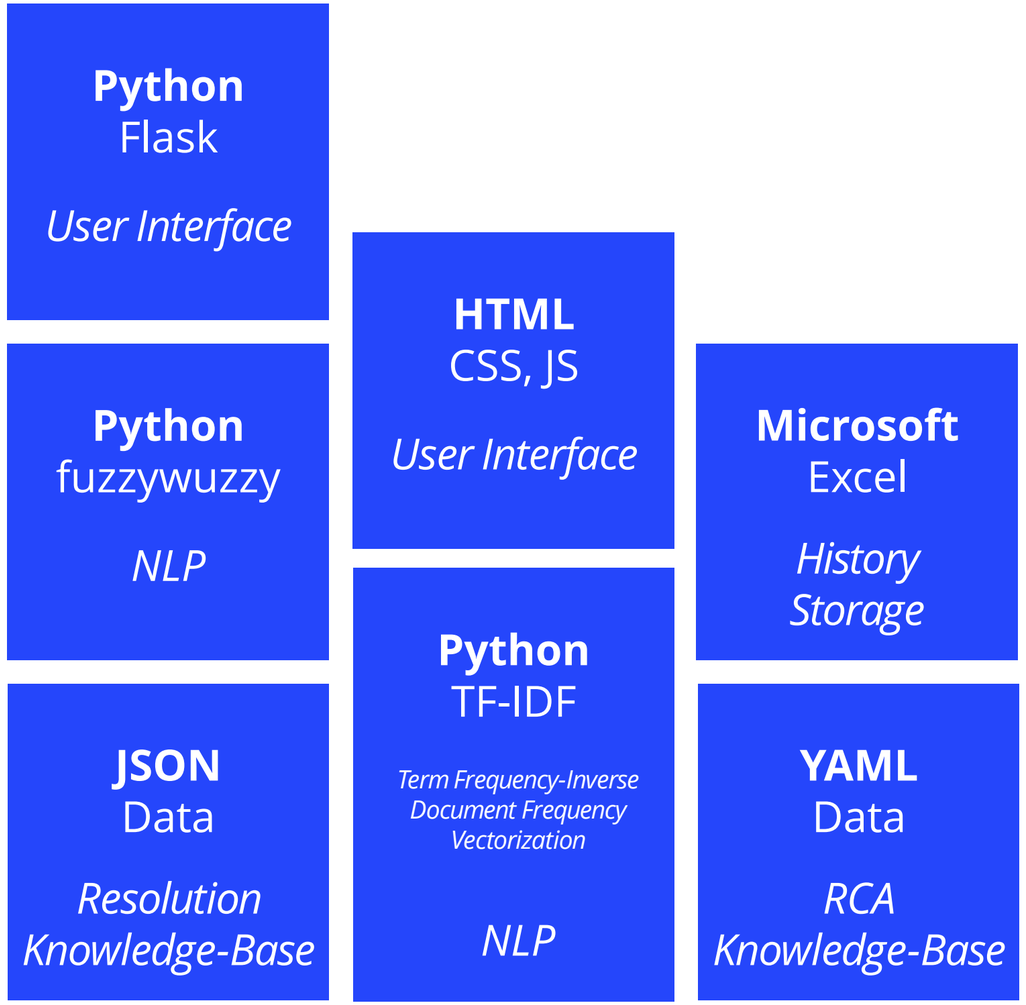
SelfHeal Technology —

SituationPlanet

SITUATIONPLANET

Technology Stack

- The 'SituationPlanet' technology stack encompasses a backend built with Python and Flask for interactive user interfaces.
- Incident data is stored in non-relational databases like Excel, JSON and YAML while AI/ML tasks utilize libraries like scikit-learn for machine learning and natural language processing.
- The application is hosted on a personal cloud compute instance, with Docker containers managed by Kubernetes for consistent deployment. Monitoring is facilitated through the WatchDog script.
- This stack ensures efficient incident classification, root cause analysis, resolution suggestions, and user-friendly interactions in the 'SituationPlanet' solution.



Thank You

SituationPlanet
a solution by Aaditya Rengarajan

21Z02@psgtech.ac.in
+91 94445 11430