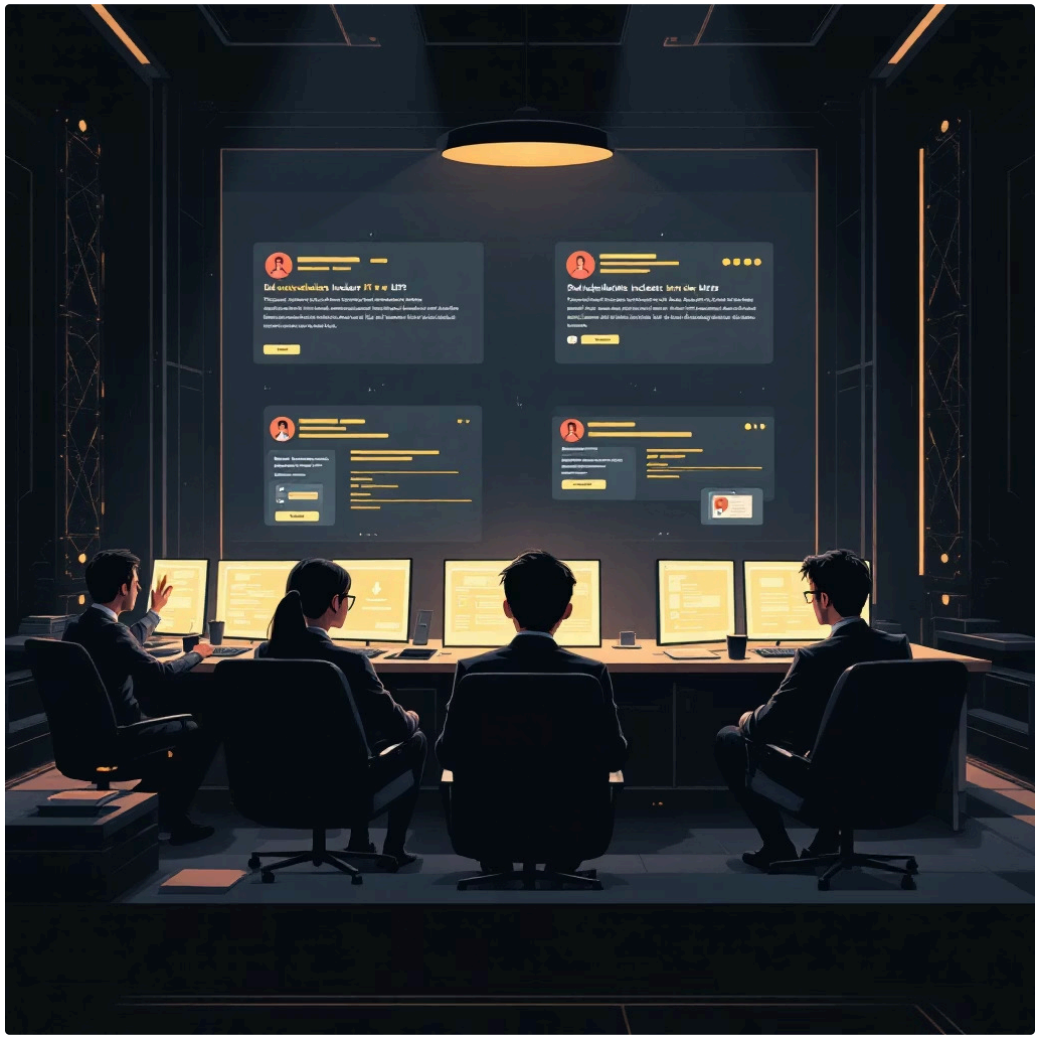
Automated Major Incident Detection & Correlation System

Using n8n + ServiceNow (Demo via Google Sheets)

Proactive detection, correlation, and automated major incident creation based on real-time incident patterns

View Demo

What Problem Are We Solving?



Current Challenges in ServiceNow Incident Management

- Multiple teams often raise **duplicate incidents** for the **same server/system issue**.
- These incidents reach different queues (Network, Unix, Database, etc.).
- This delays correlation and slows overall incident resolution.
- Major Incident process is **fully manual** → leads to delays in:
- Identifying the pattern
- Declaring the Major Incident
- Updating all related child incidents

What We Want to Achieve

01

Monitor New Incidents

Continuously track every incident created in ServiceNow in real-time

02

Check for Patterns

Identify similar incidents for the same server or system component

03

Threshold Detection

When count exceeds threshold (3 or 5), trigger automation logic

04

Create Major Incident

Automatically generate MI and attach all related child incidents

05

Update & Maintain

Continuously update MI summary as new related incidents arrive

The system intelligently reuses existing Major Incidents instead of creating duplicates, marking each child incident with `is_major_child = Yes` and the corresponding `parent_mi_number`.

Why This Helps the Business

Faster Correlation

Dramatically reduced Time to Detect (TTD) through automated pattern recognition across all incident queues

Consistent Process

Eliminates manual effort of finding similar incidents and ensures standardized Major Incident handling

Improved MTTR

Reduces SLA breaches and Mean Time to Resolve through immediate team coordination

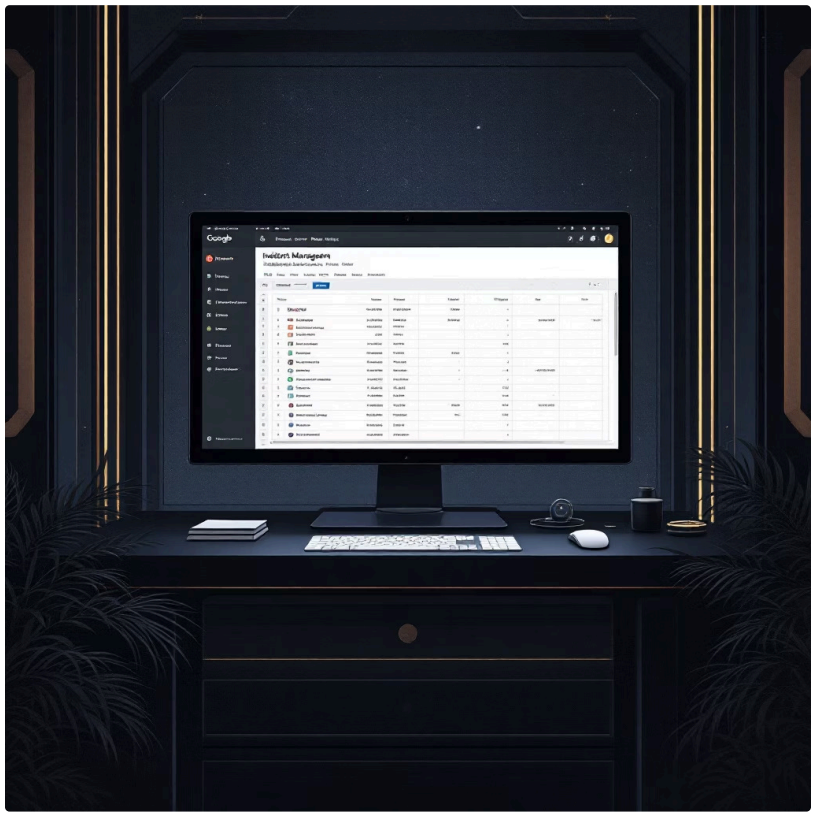
Better Experience

Enables proactive operations and delivers superior customer experience through rapid response

Why POC Using Google Sheets?

Reason for Using Spreadsheet Instead of ServiceNow API

- We do not yet have a ServiceNow API key & access token
- Google Sheets allows:
  - CRUD operations like a database
  - Easy visualization
  - Fast prototyping
  - Same logic can be replicated 1:1 to ServiceNow API once access is available
- n8n supports both Google Sheets & ServiceNow API in the same workflow model



Technologies Used

n8n Workflow Automation

Powerful workflow tool with nodes, triggers, expressions, and JavaScript-based logic for complex automation

JavaScript (ES6)

Advanced scripting inside n8n Function nodes for data processing and business logic

REST API Principles

Used in ServiceNow production version for seamless integration and data exchange

Google Sheets API

Simulated database for rapid prototyping and testing automation workflows

OpenAI Integration

Optional AI-powered generation of human-friendly response summaries for stakeholders

Workflow Architecture Overview

The workflow follows a logical sequence from incident receipt through pattern analysis, threshold checking, and Major Incident creation. Each node performs specific functions with data flowing seamlessly between steps.

Step-by-Step Workflow Logic (Part 1)

Receive Incident

Webhook trigger receives new incident data (API-triggered in ServiceNow production)

Load Configuration

Reads threshold settings and routing rules (e.g., threshold = 3 incidents per server)

Get All Incidents

Retrieves entire Incidents sheet to simulate fetching open incidents from ServiceNow

Generate Incident Number

Auto-generates INC numbers for demo (ServiceNow generates automatically in production)

Append New Incident

Prepares incident fields and appends to Google Sheet (simulates SNOW insertion)

Analyze Patterns

Checks incident count per server and returns list of server-specific incidents

Major Incident Logic (Part 2)

1

Get Existing Majors

Reads MajorIncident sheet to fetch all existing MIs from system

2

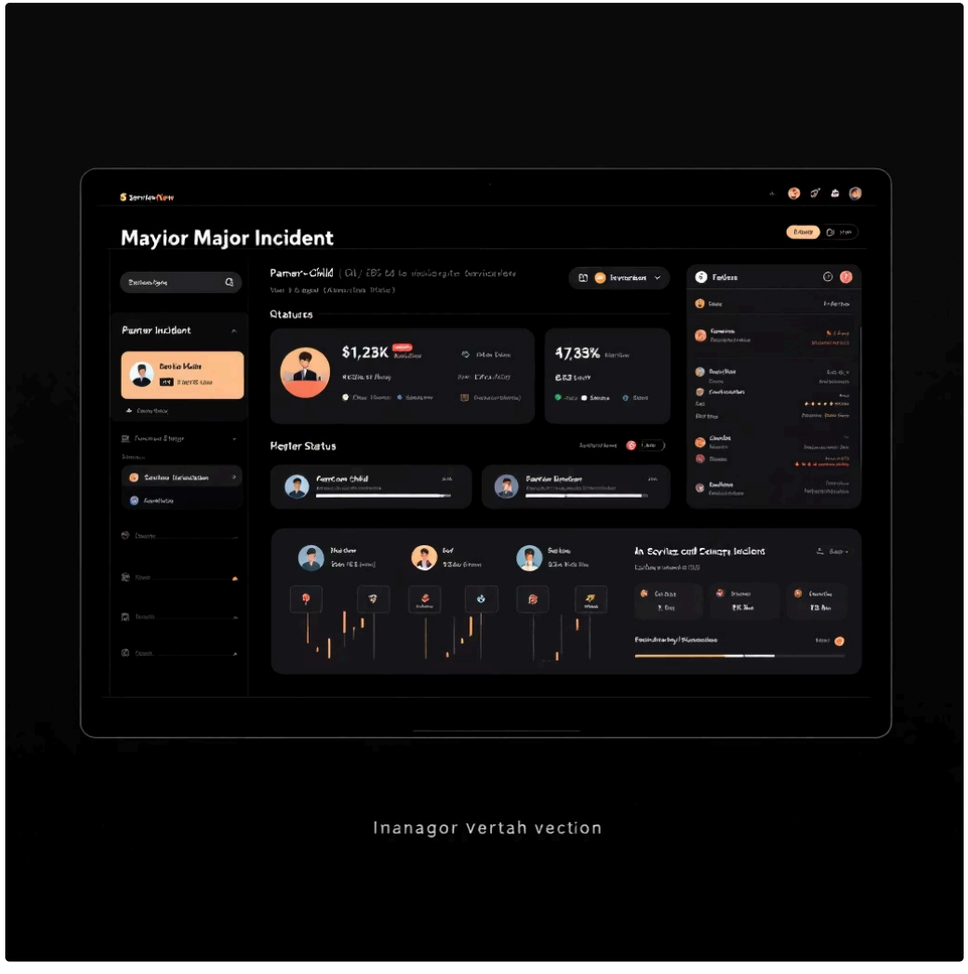
Generate Major Incident

JavaScript logic reuses open MI if exists, or generates new MI number with complete summary

3

Append or Update MI

If new MI, appends row; if existing MI, updates summary and child incident list



Updating Child Incidents

The system prepares child updates by marking `is_major_child = Yes` and setting `parent_mi_number`. All rows in the Incidents sheet are updated, including the latest incident, simulating ServiceNow PATCH API calls.

Key Innovations & Next Steps

Fully Automated

End-to-end MI creation with real-time pattern detection and auto-updating summaries

Multi-Team Consolidation

Eliminates duplicates by reusing major incidents and consolidating cross-team efforts

Modular Design

Plug directly into ServiceNow APIs when access is available—logic remains identical

---

Impact Summary & Benefits to Leadership

- Faster Major Incident declaration with improved operational visibility
- Higher customer satisfaction (CSAT) through reduced response times
- Reduced manual effort by L2/L3 teams, increasing productivity
- Scalable, reusable automation architecture extendable to Change, Problem, and CMDB

Next Steps Forward

Request ServiceNow API access to convert spreadsheet-based POC to production-ready SNOW API automation. Future enhancements include auto-closure logic, linking with Change or Problem records, and notification/alerting integrations.