Incident Response Autopilot using Agentic AI

IBM Dev Day Hackathon

AI Demystified – From Idea to Deployment

Team Name: ByteBlue

Harrison Jones
Mishal VS
Sharda Sah
Felix Kipkorir
Rahber Islam

Submission for IBM Dev Day Hackathon

Abstract

Modern enterprises increasingly rely on complex, distributed digital systems to deliver seamless customer experiences. When system incidents such as outages, performance degradation, or security anomalies occur, they directly impact business continuity, customer trust, and operational efficiency. Traditional incident response processes are often manual, reactive, and heavily dependent on human judgment. As a result, organizations face delayed response times, inconsistent severity assessment, and increased operational risk during critical incidents.

This project presents an AI-powered *Incident Response Autopilot* built using IBM watsonx Orchestrate. The solution leverages agentic AI to automate the end-to-end incident response lifecycle, including incident intake, severity classification, action execution, and final reporting. Natural language incident descriptions are analyzed by collaborating AI agents that reason over the input, determine the appropriate severity level (P1, P2, or P3), and trigger predefined response actions such as incident ticket creation and on-call team notification.

By utilizing IBM watsonx Orchestrate's agent framework and agentic workflows, the system demonstrates how AI agents can move beyond passive assistance to actively orchestrating operational processes. The solution enables faster incident triage, consistent decision-making, and reliable execution of response actions, reducing manual overhead and improving response quality. This project highlights how enterprises can transition from reactive incident management to a scalable, intelligent, and automated response model using agentic AI.

Contents

1. Introduction

Modern digital platforms operate in highly dynamic and distributed environments where system reliability and availability are critical to business success. Enterprises increasingly depend on complex application ecosystems to deliver real-time services, and even minor disruptions can quickly escalate into significant customer dissatisfaction, revenue loss, and reputational damage. Incidents such as service outages, latency spikes, data pipeline failures, or security anomalies are therefore not merely technical issues, but business-critical events that demand immediate and effective response.

Despite significant advances in monitoring and observability tools, many organizations continue to rely on largely manual incident response workflows. When an incident occurs, engineers must interpret unstructured incident reports, assess severity, create incident tickets, notify on-call teams, and coordinate mitigation efforts—often under extreme time pressure. These manual processes introduce delays, inconsistent prioritization, and dependence on individual experience, which increases operational risk during high-severity incidents.

Agentic artificial intelligence presents an opportunity to transform incident response from a reactive, human-driven process into an intelligent, automated, and consistent workflow. By enabling AI agents to reason, decide, and act within defined enterprise controls, organizations can automate incident triage, severity classification, and response execution while preserving auditability and governance. This project explores how agentic AI, implemented using IBM watsonx Orchestrate, can streamline incident response and improve operational resilience in modern enterprises.

2. Problem Statement

When incidents occur in production systems, organizations are required to respond rapidly and accurately to minimize customer impact and operational disruption. However, in many enterprises, incident response remains heavily manual and dependent on human judgment. This results in several recurring challenges:

- **Manual interpretation of incident reports:** Incident descriptions are often unstructured and require engineers to extract critical information under time pressure.
- **Inconsistent severity assessment:** Severity classification varies based on individual experience, leading to mis-prioritization of incidents.
- **Delayed escalation of critical incidents:** High-severity issues may not be escalated immediately, increasing downtime and business risk.
- **High cognitive load on on-call engineers:** Engineers must simultaneously analyze, decide, communicate, and act, increasing the likelihood of errors.
- **Fragmented tooling and workflows:** Ticketing systems, alerting platforms, and communication tools are often disconnected, slowing coordination.

These challenges result in prolonged response times, increased system downtime, and degraded customer experience. As digital systems grow in complexity and scale, manual incident handling becomes increasingly unsustainable.

There is a clear need for an intelligent, automated system that can *reason* over incident information, *decide* on appropriate severity and response actions, and *execute* those actions consistently. Such a system must operate within enterprise governance standards while reducing operational overhead and improving response reliability.

3. Solution Overview

To address the challenges of manual and fragmented incident response, we developed an **Incident Response Autopilot** using **IBM watsonx Orchestrate**. The solution leverages agentic AI to automate the end-to-end incident response lifecycle, from intake to action execution and reporting.

The system is designed to operate directly within enterprise workflows and provides the following capabilities:

- **Natural language incident intake:** Accepts unstructured incident descriptions provided by users, monitoring systems, or support teams.
- **Automated severity classification:** Analyzes incident context and assigns an appropriate severity level (P1, P2, or P3) based on impact and urgency.
- **Action orchestration through agentic workflows:** Executes predefined response actions such as incident ticket creation and on-call team notification.
- **Structured incident reporting:** Generates a concise, professional incident report summarizing severity, actions taken, and current status.

By embedding reasoning, decision-making, and action execution directly into AI agents and agentic workflows, the Incident Response Autopilot ensures fast, consistent, and auditable incident handling. This approach reduces operational overhead, minimizes response time for critical incidents, and enables enterprises to move from reactive incident management to proactive operational resilience.

4. System Architecture

The Incident Response Autopilot is implemented entirely within **IBM watsonx Orchestrate**, utilizing AI agents and agentic workflows to enable coordinated reasoning, decision-making, and action execution. The architecture follows a modular, multi-agent design that mirrors real-world enterprise incident response roles.

4.1 Agent Design

4.1.1 Incident Intake Agent

The Incident Intake Agent serves as the entry point of the system. It processes raw, unstructured incident descriptions provided in natural language and extracts relevant contextual information such as affected systems, observed symptoms, and indicators of urgency. By standardizing incoming information, this agent ensures downstream agents receive clear and consistent inputs.

4.1.2 Incident Triage Agent

The Incident Triage Agent analyzes the structured information produced by the Intake Agent and determines the appropriate incident severity level. Severity is classified according to commonly used enterprise standards:

- **P1 – Critical:** Complete service outages, widespread customer impact, or security incidents requiring immediate escalation.
- **P2 – High:** Significant performance degradation or partial service failures affecting subsets of users.
- **P3 – Low:** Minor issues, non-critical defects, or informational alerts requiring monitoring.

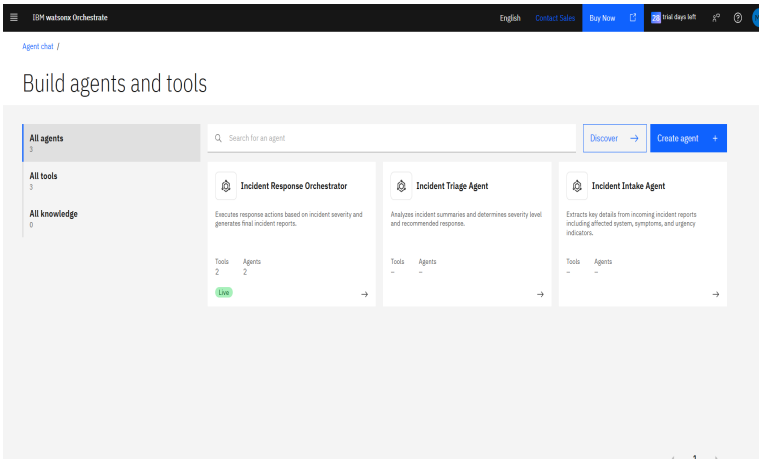
Incident Severity Levels

Severity	Description	Typical Impact	Expected Response
P1 (Critical / Priority-1)	A full-service outage or a major degradation that prevents customers from completing essential business functions.	Complete loss of revenue-generating capability, large-scale user impact, or safety/security risk.	• Create an incident ticket **and** immediately notify the on-call response team. • Activate a war-room, begin real-time monitoring, and work on rapid mitigation.
P2 (High / Priority-2)	Significant degradation affecting a sizable subset of users or a critical downstream service, but the core product still functions.	Partial loss of functionality, noticeable performance issues, or revenue impact for a segment of customers.	• Create an incident ticket. • Assign the ticket to the appropriate engineering/operations team for investigation and remediation.
P3 (Low / Priority-3)	Minor defects or cosmetic issues that do not impede core functionality or user tasks.	Small UI glitches, low-risk bugs, or non-urgent enhancements.	• Log the incident internally (e.g., in a backlog or tracking system). • Schedule for resolution in regular maintenance cycles.

This agent encapsulates decision logic, ensuring consistent and objective prioritization across all incidents.

4.1.3 Incident Response Orchestrator

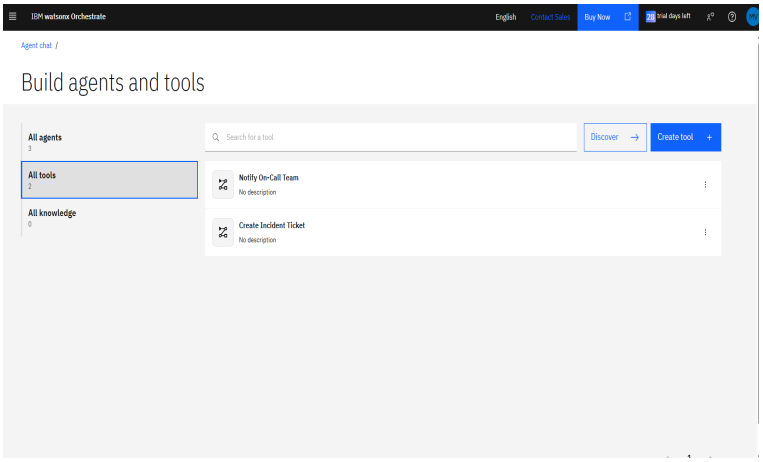
The Incident Response Orchestrator acts as the central coordinating agent. It receives the severity assessment from the Triage Agent and determines the appropriate response strategy. Based on the assigned severity, the orchestrator invokes relevant agentic workflows (tools) and generates a final, structured incident response report summarizing actions taken and current status.



4.2 Agentic Workflows (Tools)

4.2.1 Create Incident Ticket

This agentic workflow simulates enterprise ticket creation. It accepts incident details and severity as inputs and generates a professional confirmation message indicating that an incident ticket has been created. This workflow demonstrates how AI agents can trigger operational actions within structured processes.



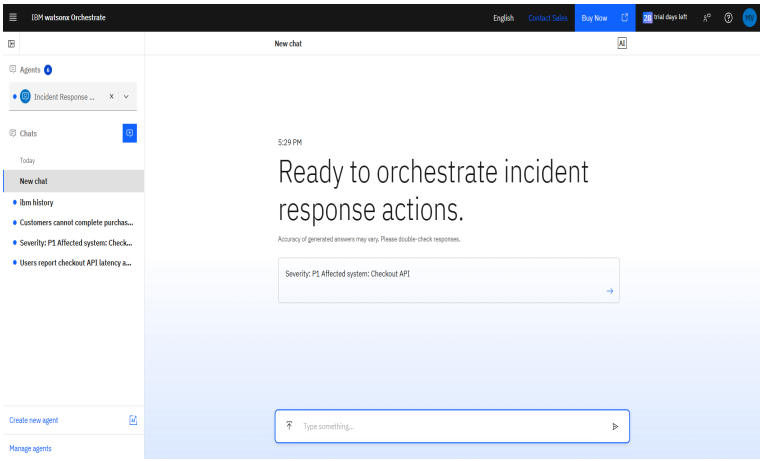
4.2.2 Notify On-Call Team

This agentic workflow simulates alerting on-call engineering or security teams for high-severity incidents. It generates confirmation messages indicating that appropriate responders have been notified, showcasing automated escalation within an incident response lifecycle.

5. End-to-End Workflow

The Incident Response Autopilot follows a fully automated, end-to-end workflow implemented using agentic orchestration in IBM watsonx Orchestrate. Each agent performs a specialized role while collaborating to achieve a common operational goal.

1. A user submits an incident description in natural language through the chat interface.
2. The **Incident Intake Agent** processes the input and extracts structured information such as affected services, symptoms, and potential business impact.
3. The **Incident Triage Agent** analyzes the extracted context and assigns an appropriate severity level (P1, P2, or P3) based on enterprise incident management standards.



4. The **Incident Response Orchestrator** evaluates the assigned severity and determines the correct response strategy. It then:
   - Executes the **Create Incident Ticket** workflow to log the incident
   - Triggers the **Notify On-Call Team** workflow for high-severity incidents
   - Generates a structured final incident report summarizing actions taken and current status

This workflow demonstrates true **agentic AI behavior**, where autonomous agents reason over information, make decisions, and execute actions without human intervention, resulting in a fast, consistent, and auditable incident response process.

6. Demonstration and Validation

The Incident Response Autopilot was validated using a diverse set of real-world incident scenarios designed to reflect common enterprise operational challenges. These scenarios covered both critical production failures and lower-severity operational issues to ensure consistent behavior across all severity levels.

The test scenarios included:

- Complete checkout service outages impacting customer transactions
- Intermittent payment gateway failures affecting international users
- Performance degradation in core services during peak traffic periods
- Security-related alerts and suspicious login activity
- Minor UI issues and scheduled batch job failures

Each scenario was submitted as a natural language input through the IBM watsonx Orchestrate chat interface. The agents autonomously analyzed the incident descriptions, determined the appropriate severity classification (P1, P2, or P3), and executed the corresponding response workflows without manual intervention.

For high-severity incidents, the system correctly escalated the issue by creating an incident ticket and simulating on-call team notification. Medium-severity incidents were logged and assigned for follow-up, while low-severity issues were documented and monitored without unnecessary escalation.

Across all test cases, the system demonstrated:

- Accurate severity classification
- Consistent and repeatable decision-making
- Reliable execution of agentic workflows
- Clear, structured final incident reports

This validation confirms that the solution can operate reliably under realistic conditions and showcases the effectiveness of agentic AI in automating enterprise incident response using IBM watsonx Orchestrate.

7. Use of IBM watsonx Orchestrate

IBM watsonx Orchestrate serves as the foundational platform for the Incident Response Autopilot. The entire solution was designed, implemented, tested, and validated within watsonx Orchestrate, demonstrating its capabilities for building production-ready agentic AI systems.

The project leverages watsonx Orchestrate in the following ways:

- **AI Agents for Reasoning and Collaboration:** Multiple specialized agents were created using watsonx Orchestrate's agent framework. Each agent is responsible for a distinct stage of the incident response lifecycle, including incident intake, severity assessment, and response orchestration. These agents reason over unstructured input and collaborate to produce consistent outcomes.
- **Agentic Workflows as Executable Tools:** Enterprise actions such as incident ticket creation and on-call team notification were implemented as agentic workflows. These workflows are executed dynamically by the agents based on incident severity, showcasing decision-driven automation rather than static rule execution.
- **Generative AI for Enterprise Responses:** Generative prompts were used within agents to produce structured, professional incident summaries suitable for enterprise operations. This ensures responses are consistent, auditable, and aligned with real-world incident management standards.
- **Built-in Testing and Evaluation:** Watsonx Orchestrate's testing and evaluation features were used to validate agent behavior across multiple incident scenarios. Test cases were executed directly within the platform, allowing the team to assess response quality, correctness, and consistency.

By using IBM watsonx Orchestrate as a unified platform for agent design, orchestration, execution, and evaluation, this project demonstrates how organizations can rapidly move from concept to deployment of agentic AI solutions. The platform enables scalable automation, reduces operational complexity, and ensures reliable incident response at enterprise scale.

8. Business Impact

The Incident Response Autopilot delivers significant and measurable value to enterprise operations by automating critical aspects of incident management. By replacing manual, error-prone workflows with agentic AI, the solution improves both operational efficiency and customer experience.

- **Reduced Incident Response Time:** Automated severity classification and action execution eliminate delays caused by manual triage and decision-making. Critical incidents are escalated immediately, reducing mean time to response (MTTR).
- **Consistent and Accurate Prioritization:** The use of AI-driven severity assessment ensures that incidents are classified consistently across teams and shifts, preventing under- or over-escalation.
- **Lower Operational Overhead:** By automating routine response actions such as ticket creation and notifications, the system reduces the cognitive load on on-call engineers and allows teams to focus on resolution rather than coordination.
- **Improved System Reliability:** Faster and more reliable incident handling minimizes downtime and service degradation, contributing to improved platform stability and resilience.
- **Enhanced Customer Experience:** Faster recovery times and reduced service disruptions directly translate into improved customer trust, satisfaction, and retention.

Overall, the solution enables organizations to shift from reactive incident handling to proactive, AI-driven operational resilience, delivering long-term business and customer value.

9. Conclusion

This project demonstrates how agentic AI can fundamentally transform traditional incident management workflows. By leveraging IBM watsonx Orchestrate, we designed and implemented a deployable, enterprise-ready Incident Response Autopilot that automates incident intake, severity classification, response execution, and reporting from end to end.

The solution highlights the practical power of agentic AI—agents are not only generating text, but reasoning over real-world incidents, making decisions, and taking concrete actions through orchestrated workflows. This approach reduces manual effort, improves consistency, and accelerates response times during critical system events.

The Incident Response Autopilot aligns strongly with the hackathon theme *"AI Demystified – From Idea to Deployment"*. It showcases a clear problem statement, a well-architected agentic AI solution, and a fully working proof of concept built entirely within IBM watsonx Orchestrate. The project demonstrates how organizations can move from concept to deployment-ready AI systems that deliver real operational impact.

Ultimately, this work illustrates how agentic AI can serve as a reliable operational partner for enterprises, enabling faster recovery, improved resilience, and better customer experiences.

References

1. IBM. *IBM watsonx Orchestrate Documentation.* https://www.ibm.com/products/watsonx-orchestrate
2. IBM. *watsonx Orchestrate – Agentic AI and Workflow Automation.* IBM Developer Documentation.
3. IBM Developer. *IBM Dev Day – AI Demystified Hackathon.* https://developer.ibm.com
4. IBM Research. *Agentic AI: Concepts and Enterprise Applications.* IBM Technical Whitepapers.
5. ITIL Foundation. *Incident Management Best Practices.* AXELOS Global Best Practices.
6. Google SRE. *Incident Response and Production Incident Management.* Site Reliability Engineering Handbook.
7. OpenAI IBM Research. *Large Language Models for Decision Support Systems.* Industry Research Publications.