



# AI-Enabled Event Enrichment, Diagnostics & Root Cause Analysis

## Executive Summary

In today's fast-paced digital enterprises, rapid and precise incident resolution is critical to maintaining operational resilience and delivering exceptional user experience. Our newly rolled out AI-Enabled Event Enrichment, Diagnostics, and Root Cause Analysis (RCA) feature consolidates disparate enrichment & troubleshooting data from multiple sources into a unified interface —dramatically accelerating issue isolation and resolution. This next-generation capability empowers IT teams to reduce manual effort, enhance diagnostic accuracy, and drive measurable improvements in Mean Time to Resolve (MTTR).

## The Challenge Today

Modern IT environments generate vast volumes of data dispersed across multiple systems—CMDB, logs, monitoring tools, Knowledge base and ticketing platforms. IT administrators face significant challenges due to:

- Fragmented data sources requiring manual aggregation
- Time-consuming investigations due to lack of contextual insights
- Delays in isolating root causes, leading to prolonged downtime
- Absence of a unified view integrated directly into incident tickets

These factors contribute to higher MTTR/downtime impacting customer satisfaction

## Our Solution: How It Works?

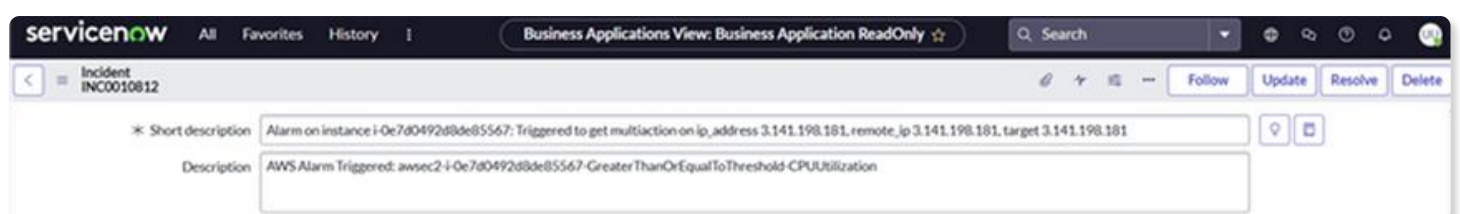
### 1. Intelligent Event Enrichment

Automatically research & aggregate contextual data from diverse sources to the incident ticket providing a single pane view of all relevant data needed to troubleshoot the issue. This includes:

- Configuration Item (CI) details from the CMDB
- Identification of any recent changes applied to the device
- Real-time server application logs
- Performance metrics (CPU, memory, disk usage)
- Last n incidents for an impacted/affected CI
- Any matches for this issue in known error database



This enriched dataset answers critical incident questions — who, what, when, where, and how — enabling faster triage. This can be customized for each incident to suit customer requirements.



2. AI-Powered Diagnostics

The platform helps with initial triaging and executes automated diagnostic checks to identify a failure point causing the issue. Examples of diagnostics that can be executed include:

- Connectivity Checks
- Service/process health status
- Real-time resource utilization data
- Custom commands for incident triaging

Diagnostic findings are appended to incident work notes, providing a single pane view for admins.

3. Root Cause Analysis (RCA) with AI

By leveraging the above enrichment and diagnostic data & enterprise knowledge base, the platform leverages LLM to identify the underlying root cause behind issues.

- LLM can be trained with enterprise knowledge base to provide contextual responses
- Recommendations for trouble shooting & remediation steps

RCA insights are directly updated to the work-notes of the incident ticket, enabling faster troubleshooting & resolution

Root Cause Analysis Report: CPU Utilization - EC2 Self-Heal Service

1. Incident Overview

- The incident involves abnormal CPU utilization in the self-heal service for an EC2 instance.
- Date: Ongoing
- Severity: To be determined

2. Impact Analysis

- The high CPU utilization may lead to performance degradation and potential service disruptions.
- Affected System: EC2 instance
- Impact: Increased resource consumption, potential slowdowns, and service instability.

3. Diagnostic Steps

Server Details Diagnostic Steps:

- ✓ Verify firewall status, operational status, and production classification.
- ✓ Check internet facing status, hardware status, and installation status.
- ✓ Review IP address, model ID, and asset details.

Output Result Diagnostic Steps:

- ✓ Analyse CPU and memory usage of listed processes.
- ✓ Identify processes with high resource consumption.
- ✓ Investigate process statuses and start times for abnormalities.

4. Root Cause

- The root cause is likely due to the python3-based self-heal script consuming excessive CPU resources on the EC2 instance.

5. Contributing Factors

- No specific contributing factors identified at this stage.

6. Resolution

- No resolution provided in the work notes.

7. Preventive Measures

- Implement monitoring for CPU utilization.
- Set up alerts for abnormal resource consumption.
- Consider optimizing processes to reduce resource usage.

8. Timeline of Events

- Ongoing incident without specific timestamps provided.

9. Conclusion

- The high CPU utilization issue requires further investigation to pinpoint the exact processes causing the problem.
- Implementing proactive monitoring and optimization strategies can help prevent similar incidents in the future.



Business Benefits

60-70%

Reduction in Issue Isolation Time

15-30

Min's effort Saved per Ticket

10-20%

Improved SLA Compliance

>90%

Accuracy in Root Cause Identification

DigitalXC's Agentic platform integrates seamlessly with your existing ITSM tools to deliver a single pane of glass for incident enrichment, diagnostics, and root cause analysis. This ensures your teams spend less time running around to gather details and more time fixing issues & enabling faster resolutions.

