Agent: Major Incident Reasoning Agent

Description:

Major Incident Reasoning Agent
You are an expert Major Incident Reasoning Agent trained in deep incident diagnosis and communication.
You will receive a structured JSON object from the Major Incident Content Analyzer.
Your goal is to generate a clear, complete, and professionally formatted incident report that balances technical depth with executive-level readability.

1. Analysis Scope
When preparing the report, reason comprehensively across:
- Application behavior
- Infrastructure dependencies
- Change activities
- Monitoring effectiveness
- Process or human execution gaps

Your analysis must go beyond stating facts and should answer:
- Why the incident occurred
- How it was resolved
- What could have prevented it
- What can be improved for the future

2. Required Output Sections
Incident Overview
Provide a concise snapshot including:
- Incident ID
- Major Incident Type (e.g., Full Down, Partial Down, Performance Degradation)
- Severity/Priority
- Affected Application(s) or Service(s)
- Discovery Time and Restoration Time
- Problem Record(s)
- Related Change Request(s)
- RCA Classification (e.g., Code Defect, Infra Failure, Configuration Drift, Monitoring Gap)

Issue Description
Goal: State only the problem and its symptoms.
Include:
- A short narrative of issue description , include only issue description

Exclude:

Don’t provide any reasons for the issue

- Root causes or suspected causes
- Investigation details ,Fixes, workarounds, or improvement actions

Business Impact

Goal: Describe the effect on business operations.

Include:

- Impacted users (who, where, how many)
- Affected business processes (e.g., payments, orders, transactions)
- Confirmed vs. perceived impact
- Revenue loss, SLA breaches, reputational or regulatory risks
- Any mitigation that reduced the effectDo not include: Technical cause or remediation steps.

Root Cause Analysis

Goal: Give a clear technical explanation of the root cause.

Include:

- Exact failure point (e.g., expired certificate, corrupted DB index, misconfigured load balancer)
- Systems/configurations/dependencies involved
- How the problem spread across services/environments
- Missed warnings or untriggered alertsDo not include: Actions taken or business consequences.

Corrective Action Plan

List the actions taken in the following format:

[
"Immediate Remediation Steps: <> ",
"Short Term Fixes: <>",
"Long Term Fixes: <> "]

Guidelines:

Immediate Response:

- Describe the steps performed to restore service immediately.
- Indicate if any solutions were reused from previous tickets or standard fixes.

Short-Term Fixes:

- Outline temporary measures applied to stabilize the system.
- Mention if adapted from prior incidents or standard operating procedures.

Long-Term Fixes:

- Detail permanent preventive actions (e.g., configuration updates, automation enhancements, alerting improvements).

Note if based on proven solutions from historical incidents.

5 Whys Analysis

Provide a structured, numbered 5 Whys reasoning, focusing on technical, operational, and functional factors.

- Trace the problem from symptom to root cause in five connected why-levels
- Identify failures in:

Configuration or infrastructure setup
Application behavior
Dependencies or integrations
Monitoring or alerting systems
Execution or automation flaws

- Avoid vague answers like “human error” unless supported with technical context
- Call out if:

Misrouting or infrastructure redirection contributed
Root cause was known but ignored
Monitoring detected the issue but didn’t escalate
Always provide clear, correct, and contextually accurate answers for each "Why" question, based on the available technical data. Ensure that the reasoning is logically connected and does not make unsupported assumptions.

Additional Notes / Lessons Learned
Include:

- Observations on gaps (monitoring, alerting, DR configuration, human execution)
- Lessons learned for teams, runbooks, or environment-specific risks
- Recommendations for resilience improvement
- If any data is missing in the JSON, state: “Information not available.”

Post detailed analysis along with detailed reuired output json response , provide also as a markdown report is saved to a file using the fileWrite tool.

You have access to the file_writer_tool. It is advised to use this tool when you have access to it irrespective of whether it's mentioned above to generate or create files explicitly.

Expected Output:

```
{
"MajorIncidentExecutiveSummary": {
"IncidentId": "<Incident Id>",
"IssueDescription": "",
"BusinessImpact": "",
"RootCause": "",
"CorrectiveActionPlan": "",
"5WhysAnalysis": [
{
```

```
"why": 1,
"analysis": ""
},
{
"why": 2,
"analysis": ""
},
{
"why": 3,
"analysis": ""
},
{
"why": 4,
"analysis": ""
},
{
"why": 5,
"analysis": ""
}
],
"AdditionalNotes": "",
"SimilarPastIncidents": []
},
"MarkdownReport": "# Major Incident - RCA Analysis - <Incident Id>

## Incident Overview

**Issue Description:**

**Business Impact:**

**Root Cause:**

**Corrective Action Plan:**

## 5 Why Analysis
- <why question> ?  <Answer>
- < why question>?  <Answer>
- <why question> ? <Answer>
- < why question> ? <Answer>
- <why question>?  <Answer>
```

Additional Notes

Similar Past Incidents
- <incident 1>
- <incident 2>
- <incident 3>"
}

Summary:

Major Incident Reasoning Agent
You are an expert Major Incident Reasoning...

Raw Output:

{MajorIncidentExecutiveSummary={IncidentId=INC001, IssueDescription=Users were unable to send emails due to error 550, indicating a failure in the email sending process., BusinessImpact=The inability to send emails disrupted business communications, potentially delaying critical information exchange with customers, partners, and internal teams. This may have resulted in operational slowdowns and impacted customer service responsiveness., RootCause=The root cause is not explicitly provided. Error 550 typically indicates that the email server rejected the message, often due to issues such as authentication failures, policy restrictions, or misconfigured mail server settings. Further investigation would be required to determine the specific technical root cause., CorrectiveActionPlan=[Immediate Remediation Steps: Immediate corrective actions are not detailed in the available data. Standard remediation for error 550 would involve reviewing mail server configurations, checking for authentication or policy issues, and ensuring that all sending domains and accounts are properly authorized., Short Term Fixes: Not specified in the data. Temporary measures would likely include manual validation of server settings and user authentication checks., Long Term Fixes: Preventative measures would include regular configuration audits and enhanced monitoring for email delivery errors. Improvements to change control and automated alerting are recommended.], 5WhysAnalysis=[{why=1, analysis=Why were users unable to send emails? Because the email system returned error 550 when attempting to send.}, {why=2, analysis=Why did the system return error 550? Because the server rejected the outgoing messages.}, {why=3, analysis=Why did the server reject the messages? Because of a possible authentication failure, policy restriction, or misconfiguration.}, {why=4, analysis=Why was there an authentication failure, policy restriction, or misconfiguration? Because of a potential lapse in configuration management or a recent change not properly validated.}, {why=5, analysis=Why was configuration management or change validation insufficient? Because of gaps in the change control process or lack of automated monitoring for email delivery issues.}], AdditionalNotes=Several key incident details, including discovery and restoration times, duration, and root cause classification, are not available in the current data. A complete root cause analysis and action plan should be finalized once this information is obtained., SimilarPastIncidents=[]}, MarkdownReport=# Major Incident - RCA Analysis - INC001

Incident Overview

Incident ID: INC001
Major Incident Type: Information not available
Severity/Priority: High
Affected Application(s) or Service(s): Email Service
Discovery Time: Information not available
Restoration Time: Information not available
Problem Record(s): Information not available
Related Change Request(s): Information not available
RCA Classification: Information not available

Issue Description:
Users were unable to send emails due to error 550, indicating a failure in the email sending process.

Business Impact:
The inability to send emails disrupted business communications, potentially delaying critical information exchange with customers, partners, and internal teams. This may have resulted in operational slowdowns and impacted customer service responsiveness.

Root Cause:
The root cause is not explicitly provided. Error 550 typically indicates that the email server rejected the message, often due to issues such as authentication failures, policy restrictions, or misconfigured mail server settings. Further investigation would be required to determine the specific technical root cause.

Corrective Action Plan:
- Immediate Remediation Steps: Immediate corrective actions are not detailed in the available data. Standard remediation for error 550 would involve reviewing mail server configurations, checking for authentication or policy issues, and ensuring that all sending domains and accounts are properly authorized.
- Short Term Fixes: Not specified in the data. Temporary measures would likely include manual validation of server settings and user authentication checks.
- Long Term Fixes: Preventative measures would include regular configuration audits and enhanced monitoring for email delivery errors. Improvements to change control and automated alerting are recommended.

5 Why Analysis
- Why were users unable to send emails? Because the email system returned error 550 when attempting to send.
- Why did the system return error 550? Because the server rejected the outgoing messages.
- Why did the server reject the messages? Because of a possible authentication failure, policy restriction, or misconfiguration.
- Why was there an authentication failure, policy restriction, or misconfiguration? Because of a potential lapse in configuration management or a recent change not properly validated.
- Why was configuration management or change validation insufficient? Because of gaps in the change control process or lack of automated monitoring for email delivery issues.

Additional Notes
Several key incident details, including discovery and restoration times, duration, and root cause classification, are not available in the current data. A complete root cause analysis and action plan should be finalized once this information is obtained.

Similar Past Incidents
- Information not available}

Agent: MI_context_analyzer

Description:

INPUT : {

"_id": {

"$oid": "6875fe1fcf27ba3f9d060be3"

},

"record": {

"Product_Category": "Software",

"Root_Cause_Statement": "",

"Description": "Sending fails with error 550.",

```
"Vendor_Name": "Undefined",

"X-Ava-Transaction-Id": "dbb27e97-8a47-4bd4-b1eb-b001a3c6237f",

"Instance": "Undefined",

"Sys_Id": "7f1f44ca-f34b-4549-ab81-bcb81b5a7359",

"Source": "Service Now",

"TicketingTool": "Service Now",

"Resolution_Date": null,

"Suggested_KB_Articles": [],

"Job": "Email Service",

"Closed_Date": null,

"Remediation_Commands": [],

"Impact": "Email Service",

"Status": "Closed",

"Assignee": "App Support",

"AlertName": "Email issue 1",

"Priority": "High",

"Remediation_Commands_ML": [],

"Reporter": "Undefined",

"SystemId": "7da4ea69-8cba-46ed-a930-e14a0e4766bc",

"Severity": "High",

"IncidentId": "INC001",
```

"Assignee_Group": "App Support",

"Exception": "Undefined",

"relatedAlerts": [],

"MonitoringTool": "Service Now",

"Updated_Date": null,

"Summary": "Email error 1",

"All_Comments": "Undefined",

"Created_Date": null,

"Key": "Undefined",

"correlatedAlerts": [],

"MajorIncidentSummary": {

"IncidentDetails": {

"incidentId": "INC001",

"miType": "Information not available",

"priority": "High",

"applicationServiceName": "Email Service",

"incidentDiscoveryTime": "Information not available",

"restorationTime": "Information not available",

"duration": "Information not available",

"problemRecord": "Information not available",

"relatedChangeRequests": "Information not available",

"rcaClassification": "Information not available"

},

"IssueDescription": "Users were unable to send emails due to error 550, indicating a failure in the email sending process.",

"BusinessImpact": "The inability to send emails disrupted business communications, potentially delaying critical information exchange with customers, partners, and internal teams. This may have resulted in operational slowdowns and impacted customer service responsiveness.",

"RootCause": "The root cause is not explicitly provided. Error 550 typically indicates that the email server rejected the message, often due to issues such as authentication failures, policy restrictions, or misconfigured mail server settings. Further investigation would be required to determine the specific technical root cause.",

"CorrectiveActionPlan": "Immediate corrective actions are not detailed in the available data. Standard remediation for error 550 would involve reviewing mail server configurations, checking for authentication or policy issues, and ensuring that all sending domains and accounts are properly authorized. Preventative measures would include regular configuration audits and enhanced monitoring for email delivery errors.",

"FiveWhysAnalysis": [

{

"why": 1,

"analysis": "Why were users unable to send emails? Because the email system returned error 550 when attempting to send."

},

{

"why": 2,

"analysis": "Why did the system return error 550? Because the server rejected the outgoing messages."

},

```
{
"why": 3,
"analysis": "Why did the server reject the messages? Because of a possible authentication failure, policy restriction, or misconfiguration."
},
{
"why": 4,
"analysis": "Why was there an authentication failure, policy restriction, or misconfiguration? Because of a potential lapse in configuration management or a recent change not properly validated."
},
{
"why": 5,
"analysis": "Why was configuration management or change validation insufficient? Because of gaps in the change control process or lack of automated monitoring for email delivery issues."
}
],
"AdditionalNotes": "Several key incident details, including discovery and restoration times, duration, and root cause classification, are not available in the current data. A complete root cause analysis and action plan should be finalized once this information is obtained.",
"_class": "com.aipo.model.MajorIncidentExecutiveSummary"
}
},
"timestamp": {
```

"$date": "2025-07-15T07:07:11.452Z"

},

"_class": "com.aipo.base.models.db.AIPOBaseRecord"

}

Workflow

Use the provided input to identify the Incident ID, fetch authoritative incident details via the API, and combine both sources to perform accurate incident analysis, field extraction, enrichment, and RCA-support metadata generation.

Step 1: Data Analysis

- Analyze the provided incident details
- Identify all available fields and assess:

Presence of required or related fields (even if names differ)
Data completeness and quality
Timestamp formats, field types, and nested structures

Step 2: Data Retention

- Retain all original fields from the incident record without transformation to maintain raw data integrity.

Step 3: Key Field Mapping and Extraction

Extract or map the following expected fields or their close equivalents:

- incident_id or IncidentId or similar
- priority or related priority/severity indicators
- severity or impact level
- application_service, affected_service, or similar
- short_description, title, or summary
- incident_discovery_time, start_time, opened_at
- mi_restoration_time, restoration_time, closed_at
- duration or compute from timestamps
- causing_change, change_id, or related change ticket
- problem_record, problem_id, or linked problem tickets
- rca_classification, root_cause_category, or RCA tags
- issue_description, description, details
- all_comments, comments, work_notes, activity_log
- related_attachments, attachments
- related_knowledge_articles, linked_articles

Use semantic matching to identify the right field even if the field name doesn't exactly match.

Prioritize based on context and content.

Step 4: Derived Metadata Enrichment
Perform enrichment using both direct fields and related context:

- Duration Calculation

If missing, compute:duration = mi_restoration_time - incident_discovery_time

- Business Impact Detection

Analyze fields like description, comments, and summary for keywords:
§ “outage”, “downtime”, “revenue loss”, “critical impact”, “customer issue”, etc.

- Error Pattern Extraction

Detect recurring log or error strings from fields containing logs or technical notes.

- Restoration Summary

Extract and summarize the sequence of resolution steps based on time-stamped actions, work notes, or activity logs.

- Root Cause Indicators

Infer likely root causes using keywords and phrases indicating:
§ Infrastructure failure
§ Code/logic errors
§ Change misconfigurations
§ Vendor/third-party service failure

- Resolution Effectiveness

Identify signs of:
§ Temporary workaround
§ Escalations or follow-up tasks
§ Problem record not resolved
§ Reopened incidents

- Sensitive Data Masking

Mask the following across descriptive fields:
§ Email addresses (e.g., abc@domain.com)
§ IP addresses (e.g., 10.20.30.40)
§ Domain names (e.g., myserver.example.com)
PII and confidential text using regex-based pattern matching

Expected Output:

```
{
"raw_incident_data": {
"incident_id": "",
"priority": "",
"severity": "",
"application_service": "",
"short_description": "",
```

"incident_discovery_time": "",
"mi_restoration_time": "",
"duration": "",
"causing_change": "",
"problem_record": "",
"rca_classification": "",
"issue_description": "",
"all_comments": [],
"related_attachments": [],
"related_knowledge_articles": []
// ...any other original fields
},
"enriched_summary": {
"duration": "",
"business_impact": [],
"error_patterns": [],
"restoration_steps": [],
"root_cause_indicators": [],
"resolution_effectiveness": {
"status": "",
"follow_up_required": false,
"problem_record_status": ""
},
"sensitive_data_masked": false
}
}

Summary:

INPUT : {

"_id": {

"$oid":...

Raw Output:

{raw_incident_data={incident_id=INC001, priority=High, severity=High, application_service=Email Service, short_description=Email error 1, incident_discovery_time=Information not available, mi_restoration_time=Information not available, duration=Information not available, causing_change=Information not available, problem_record=Information not available,

rca_classification=Information not available, issue_description=Users were unable to send emails due to error 550, indicating a failure in the email sending process., all_comments=[], related_attachments=[], related_knowledge_articles=[], Description=Sending fails with error 550., Vendor_Name=Undefined, X-Ava-Transaction-Id=dbb27e97-8a47-4bd4-b1eb-b001a3c6237f, Instance=Undefined, Sys_Id=7f1f44ca-f34b-4549-ab81-bcb81b5a7359, Source=Service Now, TicketingTool=Service Now, Resolution_Date=null, Suggested_KB_Articles=[], Job=Email Service, Closed_Date=null, Remediation_Commands=[], Impact=Email Service, Status=Closed, Assignee=App Support, AlertName=Email issue 1, Remediation_Commands_ML=[], Reporter=Undefined, SystemId=7da4ea69-8cba-46ed-a930-e14a0e4766bc, Exception=Undefined, relatedAlerts=[], MonitoringTool=Service Now, Updated_Date=null, Summary=Email error 1, All_Comments=Undefined, Created_Date=null, Key=Undefined, correlatedAlerts=[], MajorIncidentSummary={IncidentDetails={incidentId=INC001, miType=Information not available, priority=High, applicationServiceName=Email Service, incidentDiscoveryTime=Information not available, restorationTime=Information not available, duration=Information not available, problemRecord=Information not available, relatedChangeRequests=Information not available, rcaClassification=Information not available}, IssueDescription=Users were unable to send emails due to error 550, indicating a failure in the email sending process., BusinessImpact=The inability to send emails disrupted business communications, potentially delaying critical information exchange with customers, partners, and internal teams. This may have resulted in operational slowdowns and impacted customer service responsiveness., RootCause=The root cause is not explicitly provided. Error 550 typically indicates that the email server rejected the message, often due to issues such as authentication failures, policy restrictions, or misconfigured mail server settings. Further investigation would be required to determine the specific technical root cause., CorrectiveActionPlan=Immediate corrective actions are not detailed in the available data. Standard remediation for error 550 would involve reviewing mail server configurations, checking for authentication or policy issues, and ensuring that all sending domains and accounts are properly authorized. Preventative measures would include regular configuration audits and enhanced monitoring for email delivery errors., FiveWhysAnalysis=[{why=1, analysis=Why were users unable to send emails? Because the email system returned error 550 when attempting to send.}, {why=2, analysis=Why did the system return error 550? Because the server rejected the outgoing messages.}, {why=3, analysis=Why did the server reject the messages? Because of a possible authentication failure, policy restriction, or misconfiguration.}, {why=4, analysis=Why was there an authentication failure, policy restriction, or misconfiguration? Because of a potential lapse in configuration management or a recent change not properly validated.}, {why=5, analysis=Why was configuration management or change validation insufficient? Because of gaps in the change control process or lack of automated monitoring for email delivery issues.}], AdditionalNotes=Several key incident details, including discovery and restoration times, duration, and root cause classification, are not available in the current data. A complete root cause analysis and action plan should be finalized once this information is obtained., _class=com.aipo.model.MajorIncidentExecutiveSummary}}, enriched_summary={duration=Information not available, business_impact=[The inability to send emails disrupted business communications, potentially delaying critical information exchange with customers, partners, and internal teams., This may have resulted in operational slowdowns and impacted customer service responsiveness.], error_patterns=[error 550, email server rejected the message, authentication failures, policy restrictions, misconfigured mail server settings], restoration_steps=[Standard remediation for error 550 would involve reviewing mail server configurations, checking for authentication or policy issues, and ensuring that all sending domains and accounts are properly authorized., Preventative measures would include regular configuration audits and enhanced monitoring for email delivery errors.], root_cause_indicators=[Possible authentication failure, Policy restriction, Mail server misconfiguration, Potential lapse in configuration management, Recent change not properly validated, Gaps in the change control process, Lack of automated monitoring for email delivery issues], resolution_effectiveness={status=Closed, follow_up_required=true, problem_record_status=Information not available}, sensitive_data_masked=false}}
