# Integrating GenAI with Splunk to Drive Digital Transformation

PLA1423

Technical Session
September 2025

.conf25
splunk>

# Forward-looking statements

This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. We undertake no obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

splunk> .conf25

# Table of Contents

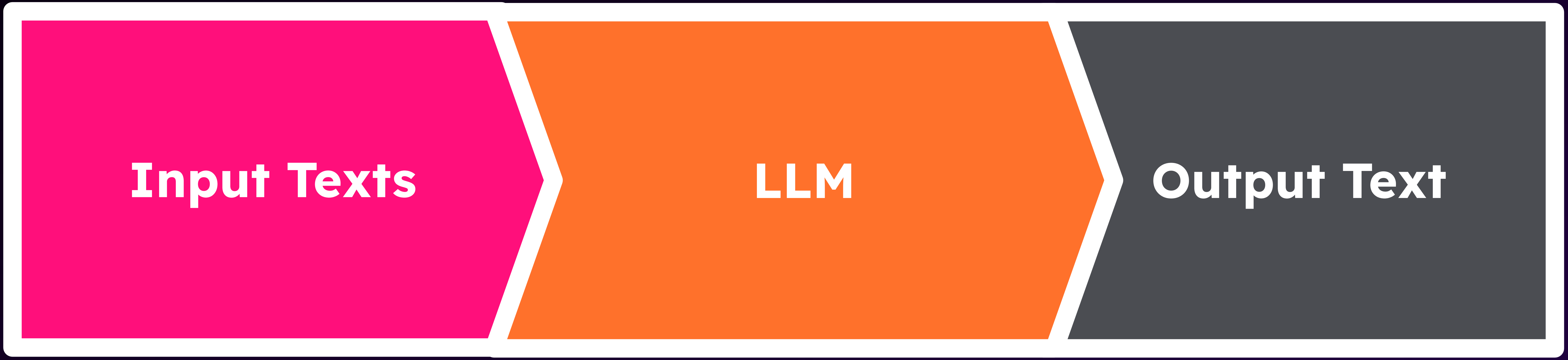
1. Large Language Models
2. Adapting current processes with LLM
3. Use-Case 1: Splunk Health Monitoring
4. Use-Case 2: Chatbot
5. Technical Overview
6. Unlocking the Next Chapter with LLMs

# Large Language Models (LLM)

# Large Language Models (LLM)

Language Models (LLMs) are advanced AI systems capable of understanding and generating human-like text. They utilize vast datasets to learn language patterns, enabling nuanced comprehension and contextual understanding.

# LLM Workflow



# Adapting Current Processes with LLM

# Current Processes with LLM

### Accepting that results are not always 100%

- Important mindset for the management: LLM doesn’t have to be perfect to be valuable
- Even an 80%-accurate quick interpretation is better than having no visibility or waiting hours for a human summary.

### Faster decision-making through the use of LLM

- Management doesn’t need to know SPL or navigate dashboards. They can simply ask:
  “Are there any critical errors in the last 24 hours?”
  “Summarise the application status in the past hour”

### Bridge human workflows with automation

- Enable human decision-making without deep technical dives (natural language)
- Teams are able to immediately act on the information, closing the gap between detection and response.

# Use Case 1: Application Health Monitoring

# Demo Video

# Alert-based monitoring  - Using LLM alert when application faces error

## Purpose

- To alert application team whenever an error to the app has occurred
- Using LLM, to provide possible reason of application failure

## Value

- Quick summary to the admin; no need to access console
- Natural language - do not need to read through all the logs for error identification

## Execution

- Recurring alert that searches application for error logs hourly
- If error logs are discovered, trigger a secondary search that searches through all the error logs in the application
- LLM will summarise the findings and notify the application team
- Output via email, or telegram

# Use Case 2: Chatbot

# Demo Video

# Chatbot Idea: A Chatgpt-like interface that people can adopt and use easily.

## Purpose

- To provide a friendly-user interface for all Users to interact conversationally with the Large Language Model.
- Keeps track of the conversation to culminate insights beyond a single prompt-answer.

## Value

- Low barrier of entry for Users to use.
- Provide coherent discussion throughout the whole conversation with the user.
- Capable of being a “guide” to the user instead of a 1-shot reply.

## Execution

- Splunk Search for the particular logs to be passed to the model.
- XML Dashboard with chat interface for conversing with the model.
- Splunk Javascript for interaction with backend server for conversational history and session state management.

# Technical Overview and Tips

# Tech Stack

### Splunk

1. **Dashboards**
2. **Splunk Custom Commands**
3. Splunk Javascript

### LLM

1. **Platform - Ollama**
2. **Serverless LLM Endpoints**

### LLM Framework

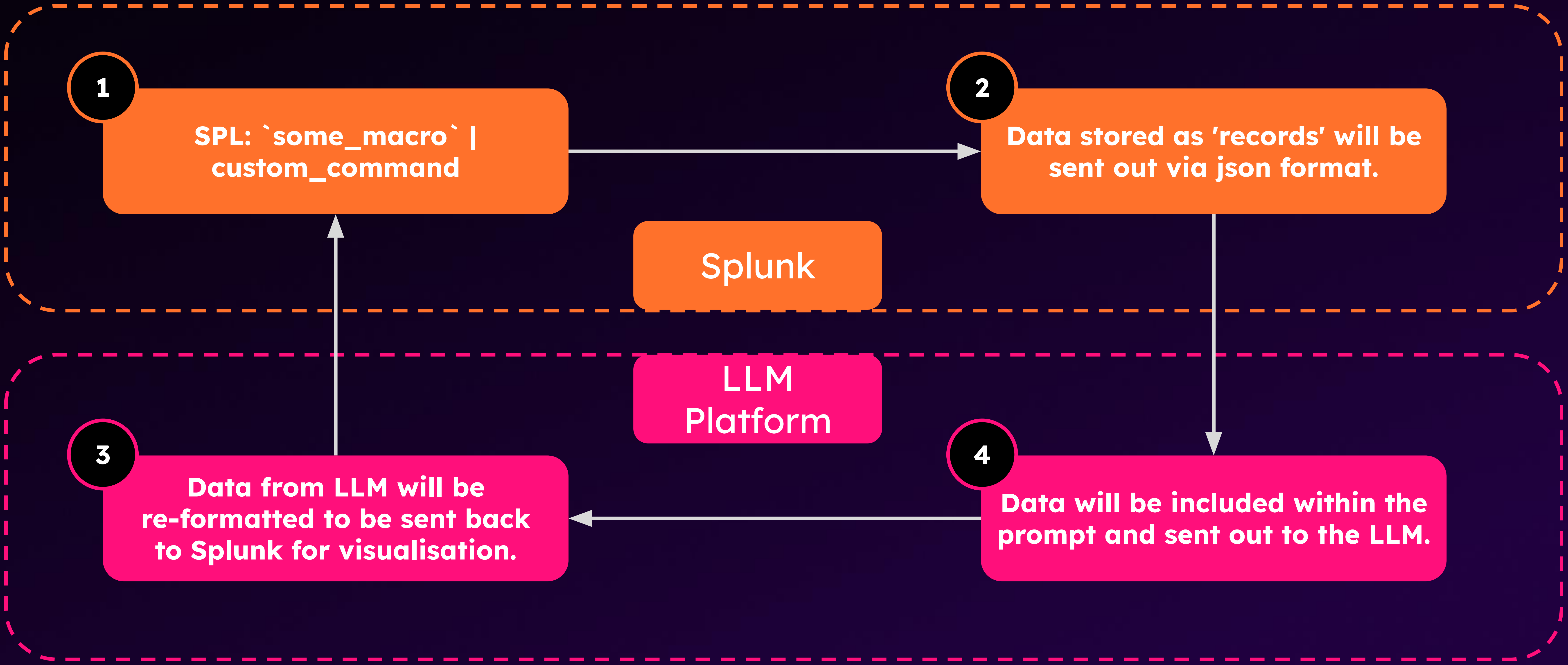
1. **LangChain**

Others:
Llamaindex

### Deployment

1. **Containers**

# Common Data Workflow



1

SPL: `some_macro` | custom_command

2

Data stored as 'records' will be sent out via json format.

Splunk

LLM Platform

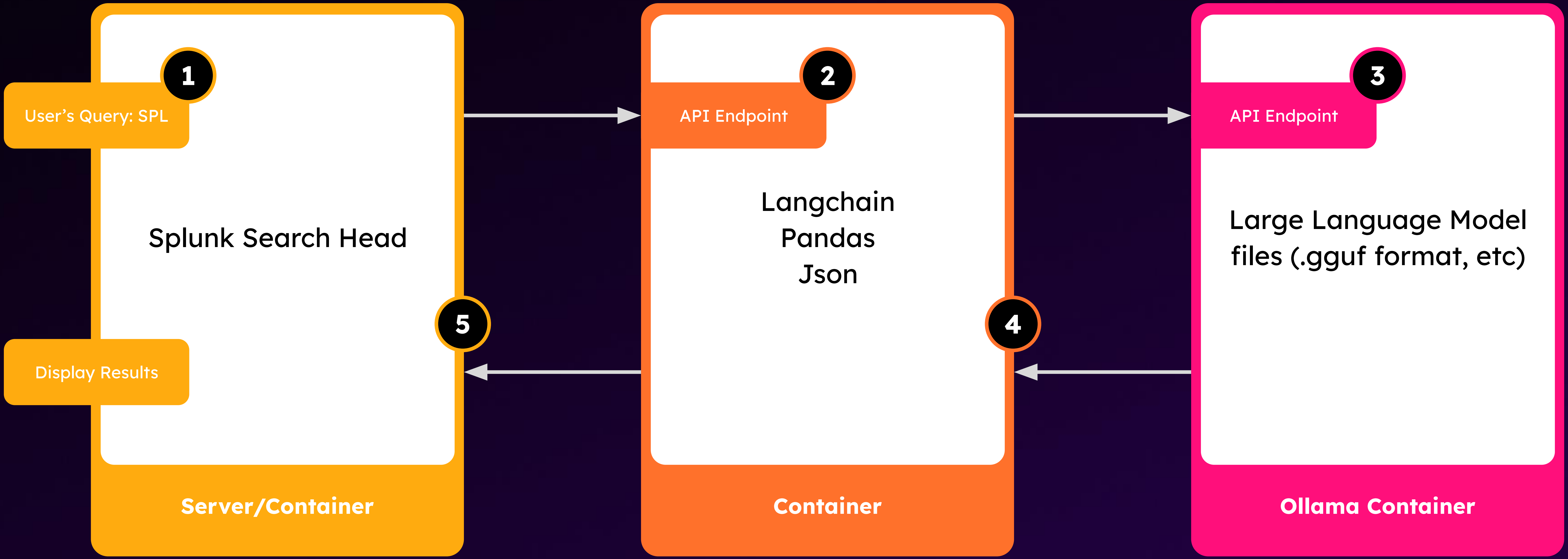
3

Data from LLM will be re-formatted to be sent back to Splunk for visualisation.

4

Data will be included within the prompt and sent out to the LLM.

# Common Architecture



# Unlocking the Next Chapter with LLMs

# Tech push operations

With the rapid evolution of LLM technology and frequent new releases, it's essential for business operations and practices to adapt, ensuring alignment with emerging capabilities and responsible adoption.

# Business & IT alignment

## Continuous Update & Delivery

1. Regularly update management on emerging GenAI capabilities and how they can enhance current business processes.
2. Proactively deliver Minimum Viable Products (MVPs) that demonstrate feasibility and business value.

## Continuous Documentation and Change Management

1. Provide clear documentation to empower both relevant business and technical teams with the knowledge and support needed to adopt GenAI tools confidently.
2. Incorporate change management practices, by consistently engaging all stakeholders, through the use of feedback loops and transparent communication.

## Consistent Multi-stakeholder Ownership

1. Ensure shared ownership of GenAI tools by aligning business goals and technical execution through ongoing collaboration between business and technical teams.

# LLM-Powered Diagnosis, Knowledge, and Execution

Mass adoption of contextual Root Cause Analysis (RCA) using LLM

Knowledge Base for Guides and Playbooks

Agentic Workflows for Operations

# LLM-Powered Diagnosis, Knowledge, and Execution

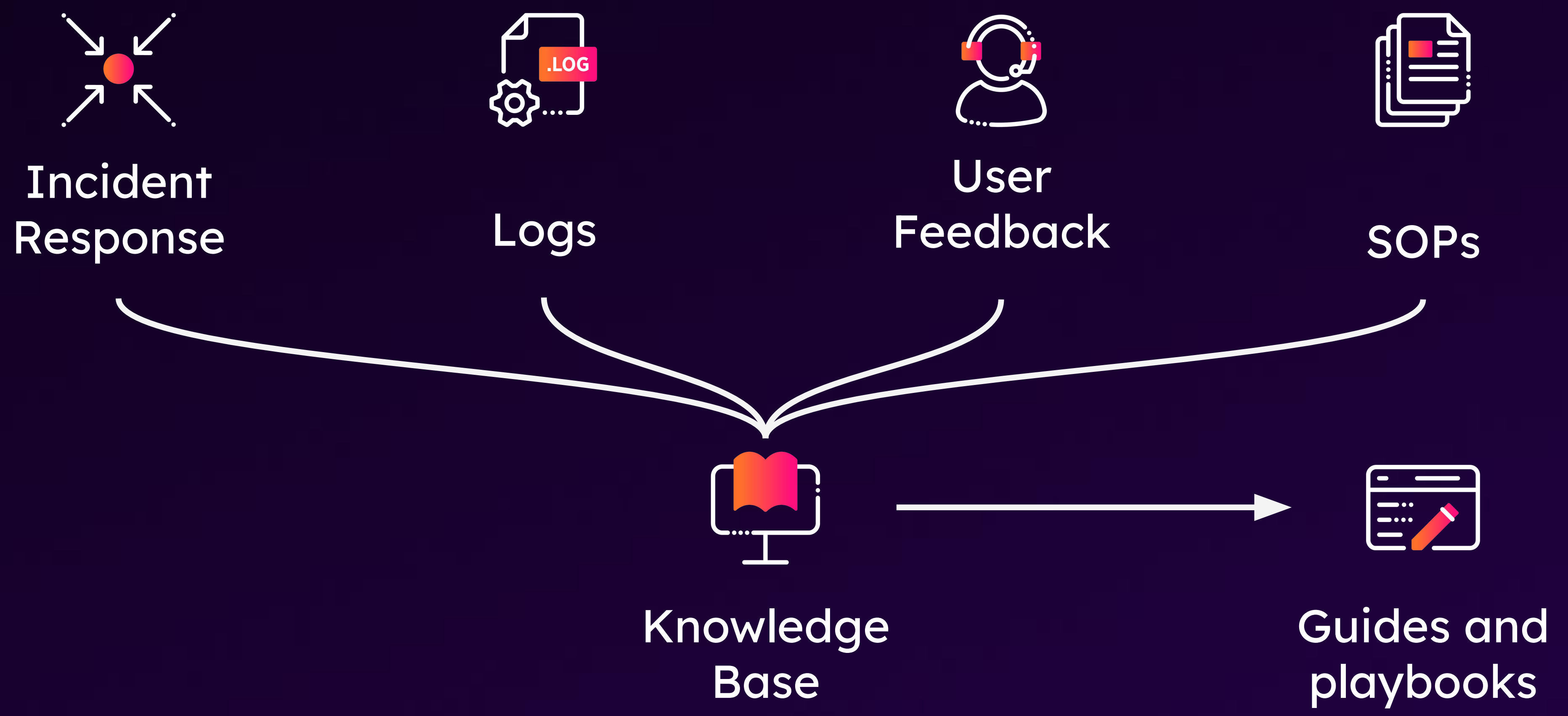
Mass adoption of contextual RCA using LLM

- Possibilities are endless – Splunk Health Monitoring is just a start
  - Applications, Servers, Dabatases
  - Ticketing investigation with ITSM such as Jira, ServiceNow
  - Cyber risk analysis & bad-actor threat investigations
- Expand RCA into every layer where data flows!

# LLM-Powered Diagnosis, Knowledge, and Execution

## Knowledge Base for Guides and Playbooks

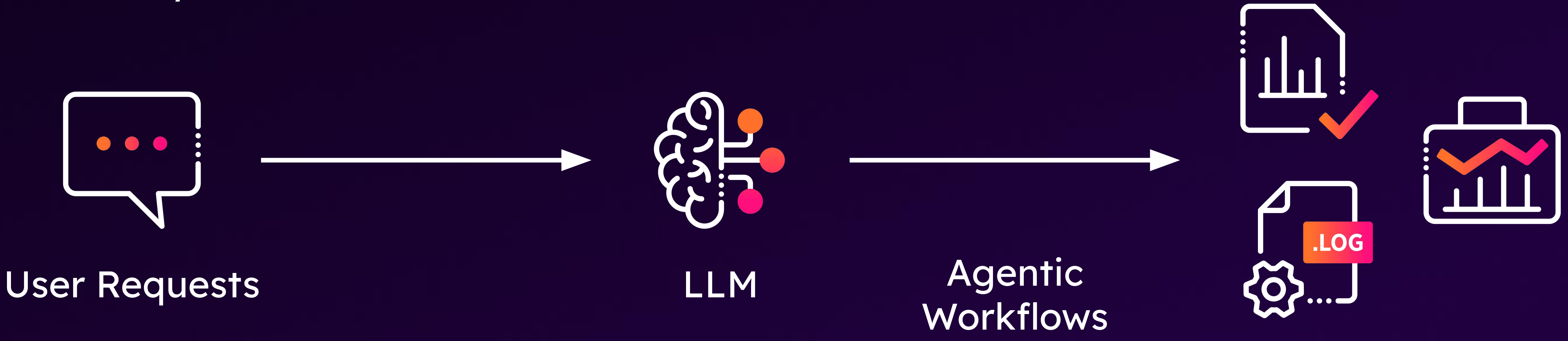
LLM can reads historical incidents, logs, user feedbacks, SOPs and store them as knowledge. This knowledge can help to generate troubleshooting guides, or remediation playbooks.



# LLM-Powered Diagnosis, Knowledge, and Execution

## Agentic Workflows for Operations

- LLM interprets and executes operational requests for Splunk Operations
  - Example: “Help to run an adhoc search to summarise the health of my application. Return the result in a dashboard and send me the link”
  - Example: “Help to onboard logs from my system to Splunk and generate routine reports”
- LLM translates intent, and create an Agentic workflow which Validates & triggers automation pipelines seamlessly



# Thank you

.conf25
splunk>