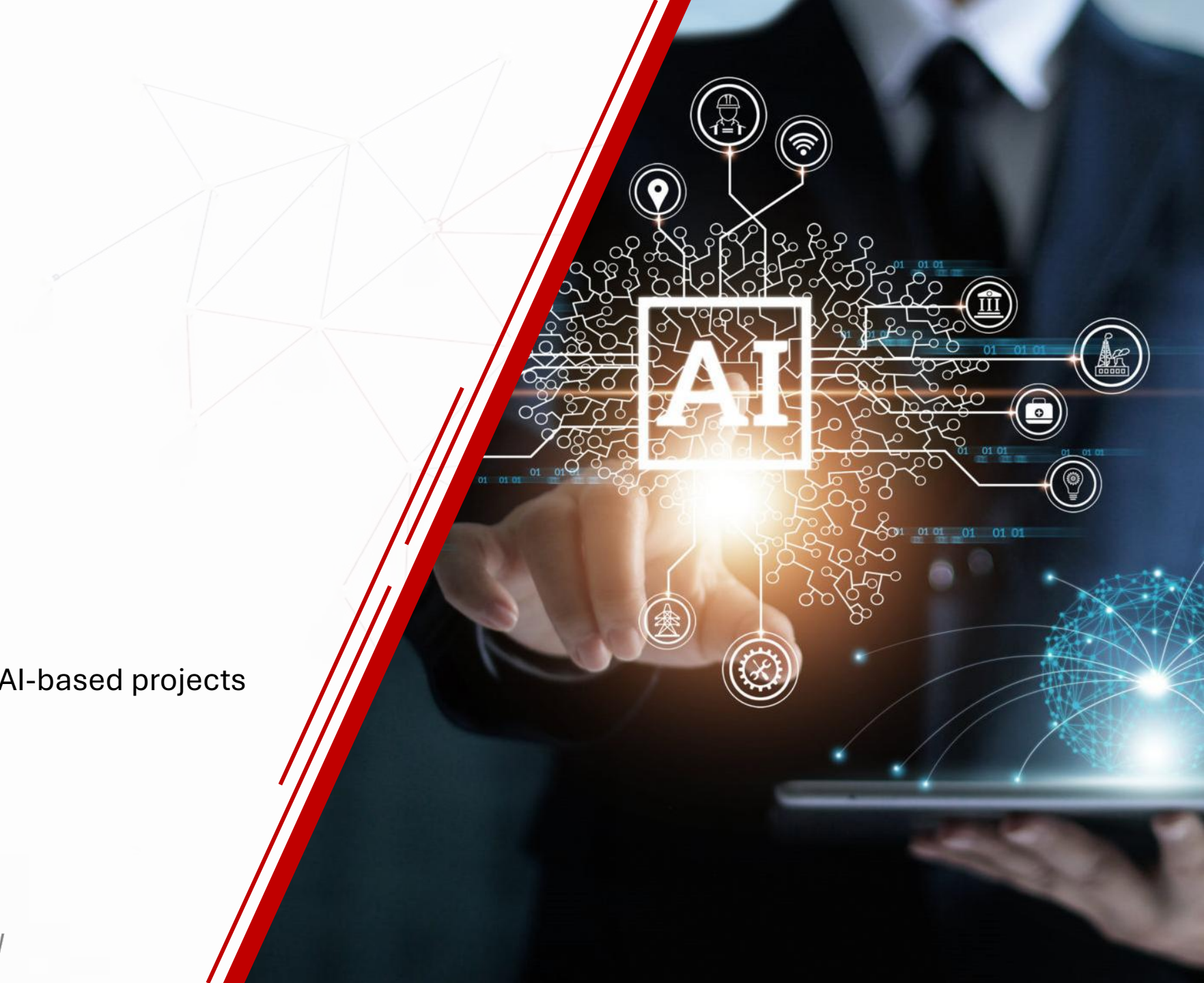# VerifAI

Validate the end-to-end lifecycle of AI-based projects
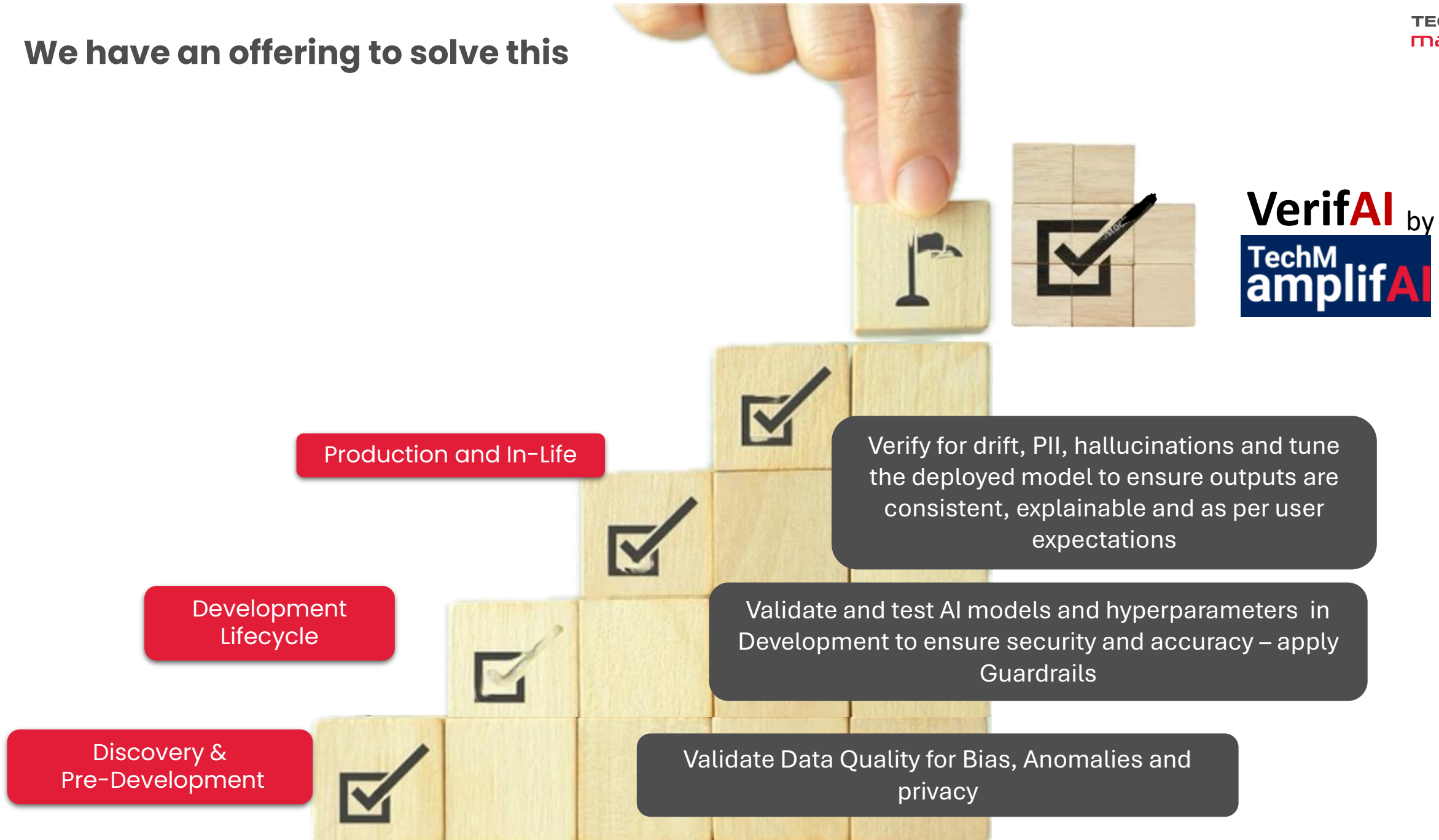
TECH
mahindra

Real Possibilities
Artificial Intelligence – The Tech Mahindra Way

We have an offering to solve this

VerifAI by
TechM amplifAI

Production and In-Life

Verify for drift, PII, hallucinations and tune the deployed model to ensure outputs are consistent, explainable and as per user expectations

Development Lifecycle

Validate and test AI models and hyperparameters in Development to ensure security and accuracy – apply Guardrails

Discovery & Pre-Development

Validate Data Quality for Bias, Anomalies and privacy

VerifAI Solution Contains a Set of Tools and APIs making it a Comprehensive LLM Evaluation Solution

TECH
mahindra

RAG Evaluation

Automate RAG evaluation with automated QnA generation and develop RAG Application with Test Driven Methodology levering automated tools

Agentic AI Evaluation*

Evaluation Agentic AI agents by measuring how the agents, tools and supervisors are performing

Load Test

Test GEN AI Application endpoints to simulate user loads and seasonality and visualize the performance

Secure Test*

Generate security attacks on Gen AI applications to prevent and test cybersecurity threats

Guardrails

Firewall Gen AI applications by Detecting and Preventing harmful prompts and cyber security attacks to safeguard the applications

Monitoring & Observability

Continuously monitor GEN AI applications for various quality metrics such as biases, hallucination, PII (and few other metrics) for timely detection of any anomalies

Playground Tools

Use specially developed tools to test how good your prompts perform before using them into your solution

Build Your Own Tools

Leverage VerifAI APIs to build your own testing, monitoring and governance solution

*Development in progress

TechM VerifAI Technical Solution

VerifAI is powered by 3 key tenets that forms its backbone

VerifAI APIs

A set of metrics APIs developed that can be used to test data before development, test the AI application during development and observability during production inferencing

Examples:
- Bias detection API
- Hallucination detection API
- Answer Relevancy API
- Context Relevancy API
- Text Similarity API
- Cohesion API

Reference Playbooks

A thorough, step-by-step guide on how validate different types of AI applications (e.g., RAG, Summarization, QnA) as well as non-functional and security testing

Examples:
- RAG Validation
- Non-Functional Validation
- Security Validation
- QnA Chatbot Validation
- Agentic AI Validation
- Vision AI Validation

Tools & Apps Powered by VerifAI

Ready to use tools and representative apps developed using VerifAI APIs to automate various testing tasks for GEN AI Applications
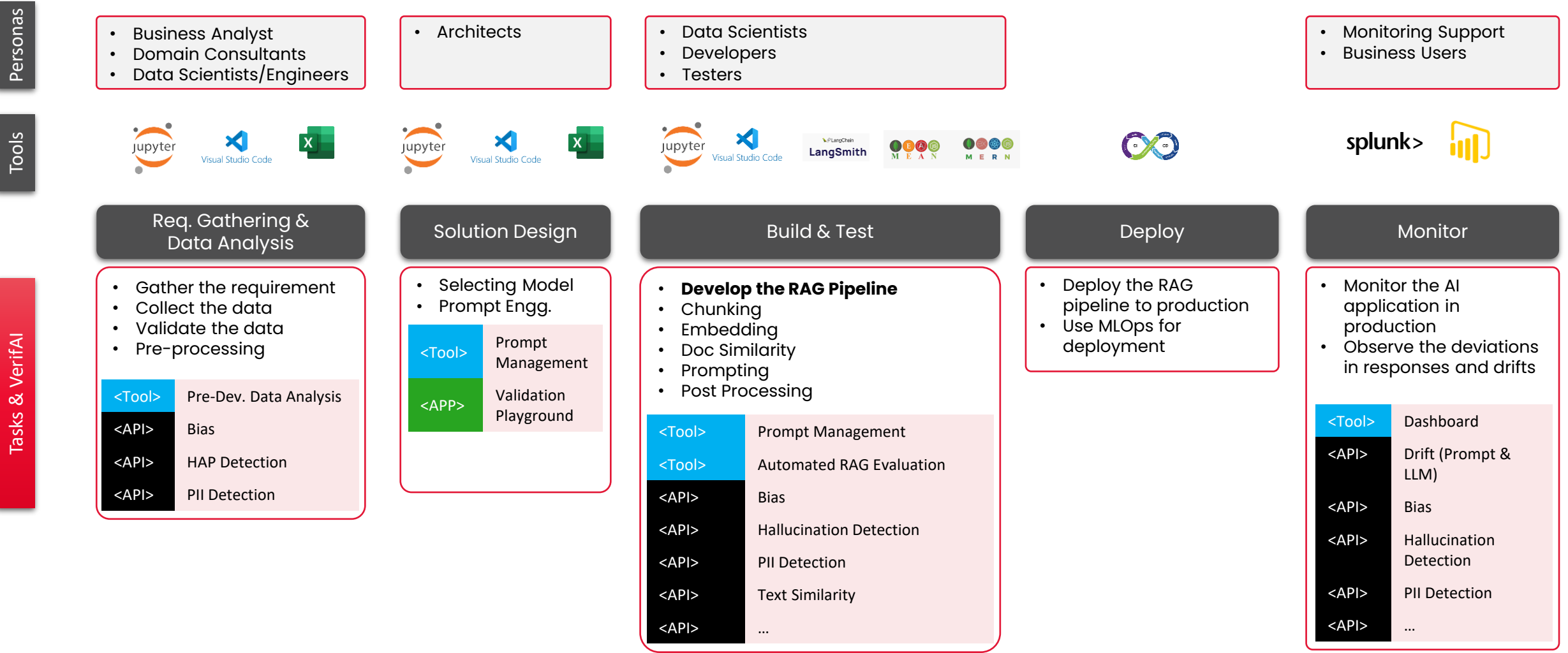
Examples:
- Automated RAG Evaluation
- Data Pre-processing
- Automated Chunking
- Automated Embedding
- Insurance Claim Conversation Agent
- Validation Playground

How VerifAI can be used across the Gen AI development cycle?

TECH mahindra

Problem Statement: Client is looking for a web-enabled chatbot powered by LLM to help Network Engineers quickly find documents, assess impact, and resolve incidents. This Gen AI based tool will streamline the process, making it easier for engineers to access the information promptly and will use RAG. By doing so, it will enhance both their speed to competency and speed to resolve

Our Approach to Develop and Test a RAG Solution:

Personas

- Business Analyst
- Domain Consultants
- Data Scientists/Engineers

- Architects

- Data Scientists
- Developers
- Testers

- Monitoring Support
- Business Users

Tools

Jupyter | Visual Studio Code | Excel

Jupyter | Visual Studio Code | Excel

Jupyter | Visual Studio Code | LangSmith | MEAN | MERN

splunk>

Tasks & VerifAI

Req. Gathering & Data Analysis

- Gather the requirement
- Collect the data
- Validate the data
- Pre-processing

<Tool>	Pre-Dev. Data Analysis
<API>	Bias
<API>	HAP Detection
<API>	PII Detection

Solution Design

- Selecting Model
- Prompt Engg.

<Tool>	Prompt Management
<APP>	Validation Playground

Build & Test

- **Develop the RAG Pipeline**
- Chunking
- Embedding
- Doc Similarity
- Prompting
- Post Processing

<Tool>	Prompt Management
<Tool>	Automated RAG Evaluation
<API>	Bias
<API>	Hallucination Detection
<API>	PII Detection
<API>	Text Similarity
<API>	...

Deploy

- Deploy the RAG pipeline to production
- Use MLOps for deployment

Monitor

- Monitor the AI application in production
- Observe the deviations in responses and drifts

<Tool>	Dashboard
<API>	Drift (Prompt & LLM)
<API>	Bias
<API>	Hallucination Detection
<API>	PII Detection
<API>	...

Clients' can derive these benefits from the solution

Open Source Based – Value for Money

- Solution based on popular open-source components
- Features such as dashboarding and documentation are also using open-source
- Seamless integration into existing technology stacks

API based Standardized Architecture

- APIs are available as RESTful APIs for easy integration during development and in production
- Standardized approach, data and schema format and documentation for developing API
- Develop the APIs in factory model based on the standardization for faster releasing of APIs

Regulatory Compliant

- Validation in the discovery and pre-development stages
- Auditable Responsible AI Systems
- Customizable schedule for verification to scale responsibly at speed.

Quicker Adoption

- Dedicated team of data scientists can be enabled on TechM VerifAI solution
- Easy-to-use APIs with playbook
- Enabled on various validation solutions from our partners

Persona Support

- Developer Personas – To score various metrics and validation during development phase
- Business Users Personas and support team Personas – To monitor the use case performance during production executions

Improved Decision Making

- Evaluating GEN AI use cases helps in identifying and addressing issues early, which can reduce development costs and improve resource allocation based on continuous performance monitoring

Compliance and Accountability

- Comprehensive logging and monitoring support regulatory compliance and traceability of data operations

Increased Efficiency

- Faster iteration cycles and improved model performance through data-driven insights enable the development of novel AI applications with greater confidence

Enhanced Data Integrity

- Regular consistency checks and result comparisons maintain high data quality, reducing the risk of errors

Cost Savings

- Identifying and addressing issues early can lead to reduced development costs as well as saving

Fostering Innovation

- GEN AI use cases drive transformation across sectors by enhancing efficiency, fostering innovation, and improving service quality

Faster Product Development

- Generative AI can accelerate the design phase and minimize unexpected late design changes, leading to more innovative designs

TECH mahindra

Disclaimer

The information is to be treated as Tech Mahindra Confidential Information. TechM provides a wide array of presentations and reports, with the contributions of various professionals. These presentations and reports may be for information purposes and private circulation only and do not constitute an offer to buy or sell any services mentioned therein. They do not purport to be a complete description of the market conditions or developments referred to in the material. While utmost care has been taken in preparing the above, we claim no responsibility for their accuracy. We shall not be liable for any direct or indirect losses arising from the use thereof and the viewers are requested to use the information contained herein at their own risk. These presentations and reports should not be reproduced, re-circulated, published in any media, website or otherwise, in any form or manner, in part or as a whole, without the express consent in writing of TechM or its subsidiaries. Any unauthorized use, disclosure or public dissemination of information contained herein is prohibited. Individual situations and local practices and standards may vary, so viewers and others utilizing information contained within a presentation are free to adopt differing standards and approaches as they see fit. You may not repackage or sell the presentation. Products and names mentioned in materials or presentations are the property of their respective owners and the mention of them does not constitute an endorsement by TechM. Information contained in a presentation hosted or promoted by TechM is provided "as is" without warranty of any kind, either expressed or implied, including any warranty of merchantability or fitness for a particular purpose. TechM assumes no liability or responsibility for the contents of a presentation or the opinions expressed by the presenters. All expressions of opinion are subject to change without notice.