**Analyze & Sort Suspicious Email Contents**

with ChatGPT

Workflow Overview

1. **Email Trigger:**
   * The workflow is initiated when an email is received via Gmail. The email trigger node monitors your Gmail inbox every minute.
2. **Email Data Extraction and Formatting:**
   * **Markdown Conversion:**  
     The email’s HTML body is converted to Markdown for improved readability by the AI.
   * **Set Email Variables:**  
     Key email fields (HTML body, subject, recipient, headers, and text body) are extracted and stored as variables using dedicated set nodes. Different nodes handle Gmail and Outlook sources.
   * **Retrieve Email Headers:**  
     An HTTP request node fetches detailed email header information (using Microsoft Graph API for Outlook), which is then formatted using a custom code node.
3. **Email Analysis Using AI:**
   * **DeepSeek R1:**  
     A DeepSeek R1 node processes the email content to produce an initial summary.
   * **AI Analysis with ChatGPT:**  
     The AI agent (using OpenAI's GPT-4o-mini model) analyzes the email's body and headers, evaluating if the email could be a phishing attempt. The output is structured in JSON, including a boolean flag (malicious) and a detailed summary.
   * **Conditional Check:**  
     An IF node examines the AI output to determine whether the email is flagged as malicious.
4. **Jira Ticket Creation:**
   * Depending on the email analysis:
     + If **malicious**: A "Potentially Malicious Ticket" is created in Jira.
     + If **benign**: A "Potentially Benign Ticket" is generated in Jira.
   * Subsequent nodes handle the attachment of email screenshots and text (converted to a file) to the Jira ticket, ensuring a comprehensive report.
5. **Additional Workflow Functions:**
   * **Pinecone and Qdrant Integration:**  
     The workflow includes nodes to interact with vector stores (like Pinecone and Qdrant) for semantic search and document processing, though these are auxiliary to the core email analysis.
   * **Google Sheets Integration:**  
     There's also a segment for retrieving or updating data in Google Sheets, which helps manage processed emails and avoid duplicates.
   * **Encryption/Decryption:**  
     To maintain security and privacy, the workflow can encrypt and decrypt email addresses before processing.
   * **Telegram Notifications:**  
     The workflow can notify via Telegram, ensuring that responsible parties are alerted when a new email has been processed and a ticket created.

Flow Summary

1. **Trigger:** Email received from Gmail.
2. **Data Extraction:** Convert email HTML to Markdown; retrieve email headers.
3. **AI Summarization & Analysis:**
   * Use DeepSeek for an initial summary.
   * Analyze email with ChatGPT to determine if it's malicious.
4. **Conditional Processing:**
   * If malicious, create a Jira ticket with the analysis and attach email screenshots and text.
   * If benign, create a separate Jira ticket.
5. **Auxiliary Nodes:**
   * Vector stores and Google Sheets nodes provide additional context and duplicate checks.
   * Encryption nodes secure sensitive data like email addresses.
   * Notifications via Telegram keep teams informed.

Customization and Use

* **System Prompts:**  
  The AI agent's system prompt is highly customizable, tailored here for a customer support scenario (Best Shirts Ltd.) dealing with order inquiries. It ensures that responses are customer-focused, factual, and efficient.
* **Jira Integration:**  
  The Jira nodes can be adjusted to match your specific project and issue types, ensuring that phishing reports or benign responses are logged correctly.
* **Security Measures:**  
  By decrypting encrypted email addresses, the workflow ensures that only authorized data is processed, preventing unauthorized queries.