**Analyze Suspicious Email Contents with**

ChatGPT Vision

Workflow Overview

1. **Email Trigger (Gmail):**
   * **Function:** Monitors a Gmail inbox for new emails using the Gmail Trigger node. Emails are fetched in real-time (polling every minute).
   * **Details:** Captures incoming email data including subject, HTML body, and headers.
2. **Variable Setup:**
   * **Set Gmail Variables:** This node extracts key email properties (HTML body, headers, subject, recipient, text content) from the Gmail Trigger's output and stores them for further processing.
   * **Set Outlook Variables:** (When enabled) Functions similarly to extract data from Outlook emails. This node is connected to a disabled Outlook trigger in this template but is provided as an option.
3. **Email Visualization (Screenshot Generation):**
   * **Screenshot HTML:** Sends the email’s HTML body to an external API ([hcti.io](http://hcti.io/)) to generate a visual screenshot of the email. This helps preserve the email's layout.
   * **Retrieve Screenshot:** Retrieves the screenshot image file, which will later be attached to the Jira ticket for visual context.
4. **Email Header Processing:**
   * **Retrieve Headers of Email:** Uses Microsoft Graph API to fetch detailed email headers (if using Outlook). The output is then formatted by the **Format Headers** code node for clarity.
   * **Set Email Variables:** These variables combine the email body and headers for further analysis by the AI agent.
5. **AI-Powered Email Analysis:**
   * **ChatGPT Analysis:** This node leverages ChatGPT (via the OpenAI API, using the GPT-4 model) to analyze the email's content and headers. It evaluates whether the email might be a phishing attempt by considering visual cues, header data, and the email body.
   * **Output:** The node generates a detailed JSON report including a summary of its findings, formatted specifically for Jira's wiki-style renderer.
6. **Automated Jira Ticket Creation:**
   * **Create Jira Ticket:** Based on the output from the ChatGPT Analysis node, this node creates a Jira ticket in a designated project (e.g., "Support") for reported phishing emails.
   * **Attachments:** The workflow also handles file attachments:
     + **Rename Screenshot:** Prepares the screenshot file by renaming it appropriately (e.g., emailScreenshot.png).
     + **Upload Screenshot of Email to Jira:** Attaches the email screenshot to the Jira ticket.
     + Additional nodes may handle the conversion and attachment of the email body as a text file.
7. **Additional Notes:**
   * **Error Handling:** The workflow includes fallback nodes and error handling measures (e.g., a NoOp node for situations where no further action is required).
   * **Customization:**
     + You can modify system messages and prompts in the ChatGPT Analysis node to fine-tune the detection criteria.
     + The integration details for Gmail, Outlook, [hcti.io](http://hcti.io/), and Jira need to be configured with your respective credentials.
     + The workflow provides clear instructions for each segment, such as how to format email data for analysis and how to structure Jira ticket details.

Data Flow Summary

1. **Email Reception:** New email arrives and is detected by the Gmail Trigger.
2. **Data Extraction:** Email content (HTML, text, headers) is extracted and stored.
3. **Visualization:** A screenshot of the email is generated via [hcti.io](http://hcti.io/).
4. **AI Analysis:** ChatGPT analyzes the email to detect phishing indicators, generating a structured report.
5. **Jira Ticket:** Based on the AI's analysis, a Jira ticket is created with the email details and attached screenshot.
6. **Review:** Security teams can then review the ticket and take appropriate action.