Unusual Login

Description:
This document describes the n8n workflow titled 'Unusual Login'. The workflow JSON has been sanitized and made paste-ready for n8n v1.110.1. Use the 'Paste JSON' feature in the n8n editor to import the workflow.

How to import (Paste JSON):
1. Open n8n and create a new workflow.
2. Click the three-dot menu in the top-right of the canvas and choose 'Paste JSON'.
3. Open the corresponding .json file and paste its contents into the dialog.
4. Click 'Import' — the workflow should appear on the canvas.

---

2. Configure API Integrations

This workflow uses several external services. Set up the following credentials:

- **GreyNoise API**
    - Required: API Key (no free tier).
    - Node: GreyNoise.
    - Auth: Generic Credential Type → Header Auth.
    - Header name: key, Value: your_api_key.
- **IP-API**
    - No authentication required.
    - Node: IP API.
    - Note: Limited to **45 requests per minute** per IP.
- **UserParser API**
    - Free tier: 500 requests/day.
    - Node: UserParser and Parse User Agent.
    - Auth: Generic Credential Type → Query Auth.
    - Query param: api_key=your_api_key.

- **Slack**
    - Node: Slack.
    - Configure your Slack credentials and set the channel (e.g., #security-alerts).
- **Gmail (for notifications)**
    - Node: Inform user.
    - Connect a Gmail account or SMTP credentials to send emails.

---

3. Set Triggers

- **Webhook Trigger** (New /login event):
    - Path: /705ca4c4-0a38-4ef8-9de9-abc8b3686dc6 (you can rename it).
    - Method: POST.
    - Integrate this webhook into your login system to send events.
- **Manual Trigger** (When clicking "Execute Workflow"):
    - Use this for **testing only**.

---

4. Database Configuration (Optional)

- Some nodes (Get last 10 logins from the same user, Query user by ID) are disabled.
- If you want to use them, connect your **Postgres database** with user login history.

---

5. Testing

- Use the Example event node for safe local testing.
- Once confirmed, enable the Webhook node and test with real login events.

---

6. Alert Flow

- Suspicious logins trigger:
    - **GreyNoise check** → classifies IP as malicious/benign.
    - **IP Geolocation** → compares with last login city.
    - **UserParser** → detects browser/device anomalies.
- Alerts are sent to:
    - **Slack** (security team).
    - **Email** (end-user, if email is available).

Notes:
- The JSON was sanitized to ensure compatibility with n8n v1.110.1: UUID node IDs, position fields, normalized credentials, and removal of unsupported options.
- If any node requires credentials (e.g., Slack, HTTP Request), re-add them in the n8n UI after importing.

Quick test curl (example for webhook-based workflows):
curl -X POST http://<n8n-host>:5678/webhook/<path> -H 'Content-Type: application/json' -d '{"user":"test","ip":"8.8.8.8"}'

Prepared for submission.