

Configuration Manual

MSc Research Project
Cyber Security

Cathal McGahan
Student ID: 23265884

School of Computing
National College of Ireland

Supervisor: Michael Pantridge

National College of Ireland
MSc Project Submission Sheet
School of Computing



Student Name: Cathal McGahan
Student ID: 23265884
Programme: Msc Cyber Security **Year:** 2025
Module: Msc Practicum/Dissertation/Thesis
Supervisor: Michael Pantridge
Submission Due Date: 11/12/2025, 2pm
Project Title: SMEs Do Not Adopt Cyber Risk Management: Evaluating Voice-Based Conversational AI as a Barrier-Reduction Solution
Word Count: 1286 **Page Count** 9

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:

A handwritten signature in black ink, appearing to read "Cathal McGahan".

Date: 07/12/2025

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	☐
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	☐
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	☐

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

AI Acknowledgement Supplement

MSC Cyber Security Thesis

Your Name/Student Number	Course	Date
Cathal McGahan (23265884)	MSc Cyber Security (MSCCYBE_JANOL24)	11/12/2025

This section is a supplement to the main assignment, to be used if AI was used in any capacity in the creation of your assignment; if you have queries about how to do this, please contact your lecturer. For an example of how to fill these sections out, please click [here](#).

AI Acknowledgment

This section acknowledges the AI tools that were utilized in the process of completing this assignment.

Tool Name	Brief Description	Link to tool
ChatGPT	Used quite extensively to help with the development of the POC, helping with Code and Prompt generation	ChatGPT (openai.com)

Description of AI Usage

This section provides a more detailed description of how the AI tools were used in the assignment. It includes information about the prompts given to the AI tool, the responses received, and how these responses were utilized or modified in the assignment. **One table should be used for each tool used.**

ChatGPT	
Used quite extensively to help with the development of the POC code (React and n8n)	
I would be here for a while listing out all the prompts used, the majority of the prompts used were seeking development guidance, debugging and some explanations over groq, llms, n8n and other various pieces. AI was also used to help develop monologue scripting and test scenarios for the POC while ChatGPT5.1 was used as a different baseline to test against, as detailed in the Evaluation section of research report. Listed below is a flavour of the types of prompts used to assist in the development and research of this project: • How do I set up n8n? • What is a n8n workflow? • How do I run n8n in a Docker container? • How do I set up Ollama locally? • How do I set up Groq? • What is RAG?	1. 1. How do I set up n8n? n8n can be installed in several ways (desktop, CLI, Docker, cloud), but the most common method for local or self-hosted use is via Node.js or Docker. Option A: Install via Node.js (local development): 1. Install Node.js (LTS version recommended). 2. Install n8n globally: 3. npm install -g n8n 4. Start n8n: 5. n8n 6. Access the UI in your browser at: http://localhost:5678 Option B: Install via Docker (recommended for production): 1. Install Docker and Docker Compose. 2. Create a directory (e.g., /n8n/). 3. Add a docker-compose.yml file (example shown in next section). 4. Run: 5. docker compose up -d 6. Access the UI at http://localhost:5678. 2. 2. What is an n8n workflow? An n8n workflow is a visual automation pipeline composed of nodes that perform specific operations. A workflow defines: • Trigger nodes (e.g., webhooks, schedules, events) • Action nodes (e.g., API calls, database operations, file transforms) • Data flows between nodes Workflows allow you to automate tasks, integrate systems, and

construct complex logic using a low-code interface.

3. 3. How do I run n8n in a Docker container?

Below is a standard docker-compose.yml for running n8n:
version: "3"

services:

n8n:

image: n8nio/n8n:latest

ports:

- "5678:5678"

environment:

- N8N_BASIC_AUTH_ACTIVE=true

- N8N_BASIC_AUTH_USER=admin

- N8N_BASIC_AUTH_PASSWORD=yourpassword

- N8N_HOST=localhost

- N8N_PORT=5678

- N8N_PROTOCOL=http

volumes:

- n8n_storage:/home/node/.n8n

restart: unless-stopped

volumes:

n8n_storage:

Then start the container:

docker compose up -d

This will make n8n available at:
http://localhost:5678

4. 4. How do I set up Ollama locally?

Ollama is a local LLM runtime that allows you to run models like Llama 3, Mistral, Gemma, etc.

Setup steps:

1. Go to <https://ollama.com/download>
2. Download and install the appropriate installer (macOS, Windows, Linux).
3. Verify installation:
4. ollama --version
5. Pull a model:
6. ollama pull llama3
7. Run a model interactively:
8. ollama run llama3

Optionally, Ollama can expose an API at http://localhost:11434 for integration with n8n, LangChain, etc.

5. 5. How do I set up Groq?

Groq is a cloud-based LLM inference platform that provides extremely fast inference via their GroqLPU hardware.

Setup steps:

1. Create an account at <https://console.groq.com>
2. Generate an API key inside the dashboard.
3. Install the official Groq Python SDK (optional for dev work):
4. pip install groq
5. Use the SDK with your API key:
6. from groq import Groq
client = Groq(api_key="YOUR_API_KEY")
response = client.chat.completions.create(
model="llama3-70b-8192",
messages=[{"role": "user", "content": "Hello"}]
)
print(response.choices[0].message["content"])

Or use Groq via REST:

```
curl https://api.groq.com/openai/v1/chat/completions \  
-H "Authorization: Bearer YOUR_API_KEY" \  
-H "Content-Type: application/json" \  
-d '{  
  "model": "llama3-70b-8192",
```

	<pre>"messages": [{"role": "user", "content": "Hello"}] }</pre> 6. 6. What is RAG? RAG (Retrieval-Augmented Generation) is an LLM architecture pattern in which a model retrieves relevant external data (e.g., documents, PDFs, databases) and uses that retrieved context to produce more accurate outputs. RAG has two major steps: 1. Retrieve: Pull relevant information from a vector database or search index (e.g., Chroma, Pinecone, Weaviate). 2. Generate: Pass the retrieved context into the LLM so that responses are grounded in facts instead of relying only on the model's internal parameters. RAG is used for: • Chatbots over private documents • Knowledge-base question answering • Enterprise AI assistants • Compliance and audit workflows It improves accuracy, reduces hallucinations, and ensures outputs remain aligned with authoritative data.
--	---

Evidence of AI Usage

This section includes evidence of significant prompts and responses used or generated through the AI tool. It should provide a clear understanding of the extent to which the AI tool was used in the assignment. Evidence may be attached via screenshots or text.

Additional Evidence:

[Place evidence here]

Additional Evidence:

[Place evidence here]

Configuration Manual

SMEs Do Not Adopt Cyber Risk Management: Evaluating Voice-Based Conversational AI as a Barrier-Reduction Solution

Cathal McGahan
23265884

1. Introduction

This Configuration Manual provides instructions for replicating the experimental setup of a voice-driven cybersecurity risk audit system. The system conducts automated interviews with small business owners, analyses security practices using AI, and generates CIS Risk Assessment Method (RAM) v2.1 Implementation Group 1 (IG1) assessment reports.

This manual assumes no prior technical knowledge. All steps required for successful replication are provided.

Note: The complete source code, n8n workflow JSON, and Excel template are submitted separately as the ICT Solution Artefact.

2. System Overview

The system consists of:

- A React web application for voice-based interviewing
- Groq Whisper API for speech-to-text transcription
- Groq LLM (gpt-oss-120b) for intelligent analysis
- n8n workflow automation (running in Docker)
- CIS RAM v2.1 IG1 Excel template for final reporting

3. System Requirements

Component	Requirement
Operating System	Windows 10/11 (developed and tested on Windows)
Docker Desktop	Version 28.4.0 (used during development)
Node.js	v22.19.0 or higher
Web Browser	Chrome, Edge, or Firefox (with microphone access)
Microphone	Any microphone (built-in or external)
Internet Connection	Required for API calls to Groq
RAM	Minimum 8GB recommended

Table 1: System Requirements

4. Prerequisites Setup

Obtain Groq API Key

The system requires a Groq API key for speech transcription and natural language analysis. API usage is charged per token, with typical costs of approximately \$0.02-0.04 per assessment.

1. Navigate to <https://console.groq.com>
2. Create account or log in
3. Navigate to API Keys section
4. Click 'Create API Key'
5. Copy generated key (not shown again)

Install Docker Desktop

Docker Desktop is required to run the n8n workflow automation container.

Download and install Docker Desktop from <https://www.docker.com/products/docker-desktop>

Install Node.js

Node.js v22.19.0 or higher is required for the React frontend application.

Download and install Node.js from <https://nodejs.org> (LTS version recommended)

5. Configuration Steps

Configure Frontend Environment

The React application requires a Groq API key in the environment file.

Navigate to the project root directory

Open the .env file

Replace INSERT-API-KEY-HERE with your actual Groq API key obtained in section 4

Example:

VITE_GROQ_API_KEY=gsk_your_actual_key_here

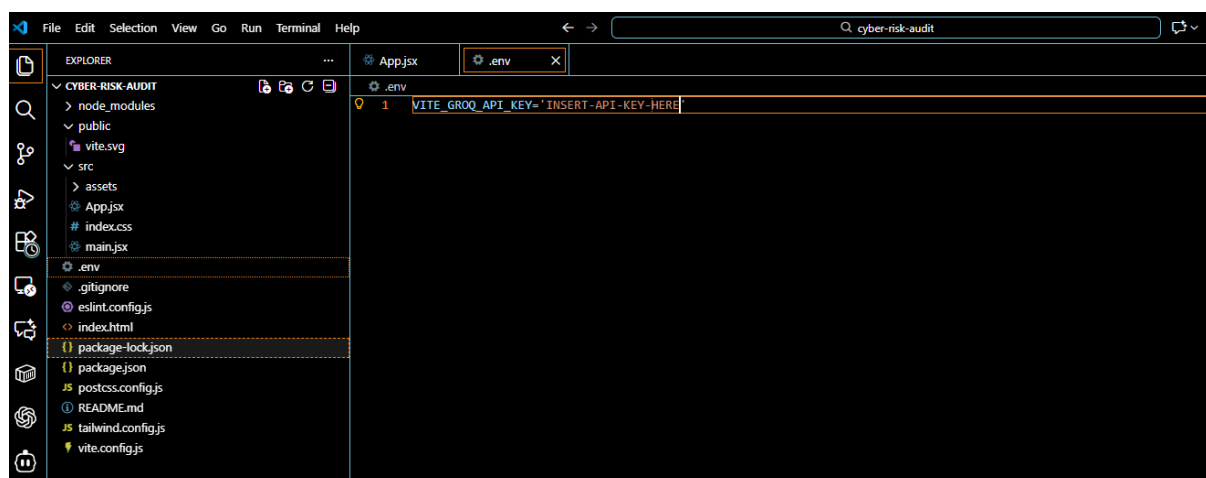


Figure 1: .env file location showing where to insert the Groq API key

Configure Docker Compose

The docker-compose.yml file is pre-configured and requires no modifications.

Configuration details:

- n8n runs on port 5678 (<http://localhost:5678>)
- Templates directory mounted to /templates in container
- xlsx library enabled for Excel manipulation

Place Excel Template

Ensure the Excel template file CIS_RAM_v2_1_for_IG1_Workbook_22_05_TEST.xlsx is located in the templates folder in the same directory as the docker-compose.yml file.

Required folder structure:

project-root/

```
├── src/
├── templates/
│   └── CIS_RAM_v2_1_for_IG1_Workbook_22_05_TEST.xlsx
├── docker-compose.yml
├── cyberRiskAuditn8n.json
├── .env
└── package.json
```

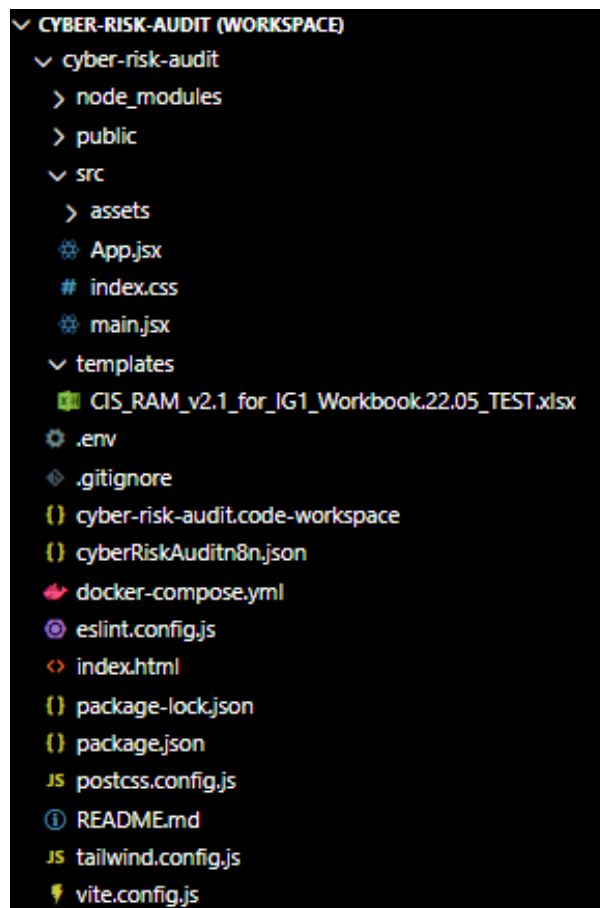


Figure 2: Project Folder Structure at time of submission

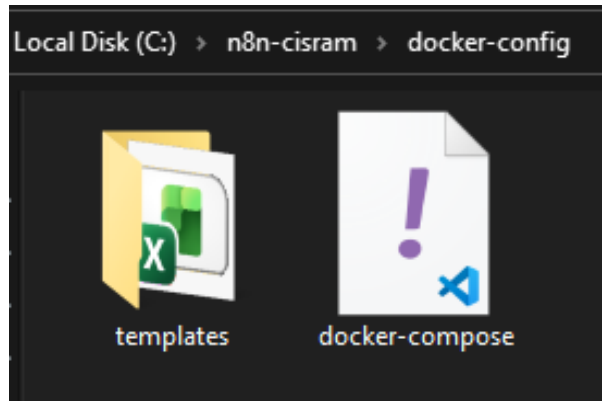


Figure 3: Folder structure showing templates folder alongside docker-compose.yml

6. Starting the System

Start n8n Container

1. Verify Docker Desktop is running (check system tray)
2. Open Command Prompt
3. Navigate to directory containing docker-compose.yml
4. Start container:

docker-compose up -d

Note: The first time you run this command, Docker will automatically download the n8n container image. This may take a few minutes depending on your internet connection.

5. Verify container is running:

docker ps

Output should show n8n container with status 'Up'.

Import n8n Workflow

1. Navigate to <http://localhost:5678>
2. Complete initial n8n setup (create owner account)
3. Click 'Import from File' or navigate to Workflows > Import from File
4. Select cyberRiskAuditn8n.json (submitted as part of ICT Solution Artefact. In project root of Code folder)
5. Activate workflow using 'Active' toggle

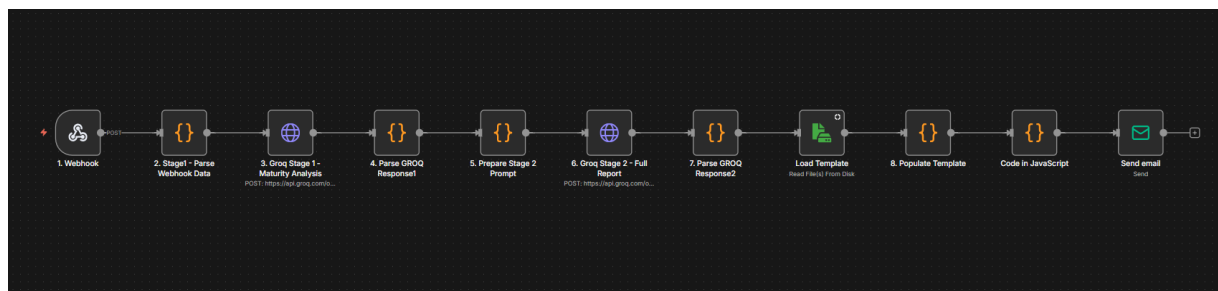


Figure 4: Complete n8n workflow showing all nodes

7. Configuring n8n Workflow Credentials

After importing the workflow, you must configure API keys and credentials. The imported workflow will not contain these for security reasons.

Configure Groq API Keys

The n8n workflow requires Groq API keys in two separate nodes.

Node 3: Groq Stage 1 - Maturity Analysis

1. In n8n, click on the "3. Groq Stage 1 - Maturity Analysis" node
2. Scroll down to "Header Parameters" section
3. Locate the "Authorization" field
4. In the "Value" field, replace the existing text with: Bearer YOUR_GROQ_API_KEY
 - Replace YOUR_GROQ_API_KEY with your actual Groq API key from section 4

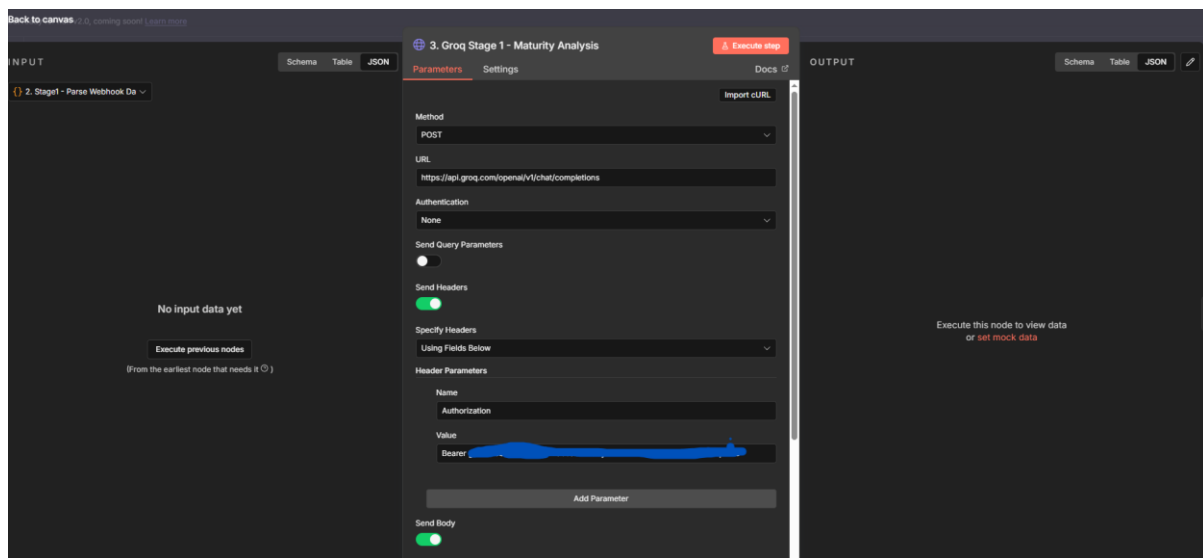


Figure 5: Groq Stage 1 node showing where to insert API key in Authorization header

Node 6: Groq Stage 2 - Full Report

1. Click on the "6. Groq Stage 2 - Full Report" node
2. Scroll down to "Header Parameters" section
3. Locate the "Authorization" field
4. In the "Value" field, replace the existing text with: Bearer YOUR_GROQ_API_KEY
 - Replace YOUR_GROQ_API_KEY with your actual Groq API key from section 4

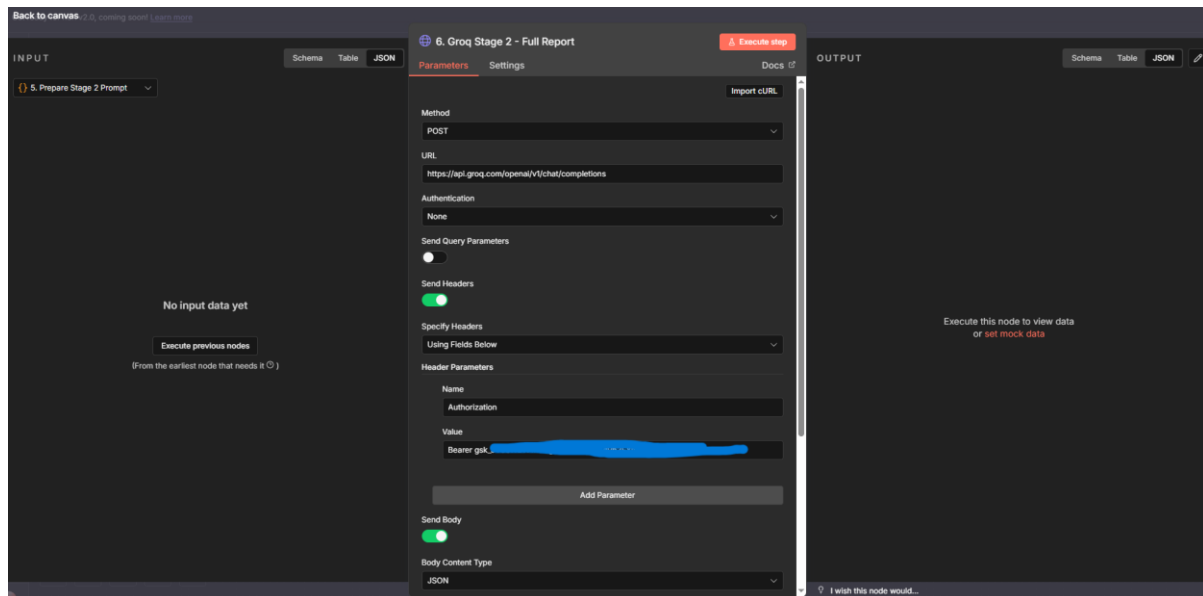


Figure 6: Groq Stage 2 node showing where to insert API key in Authorization header

Important: Use the same Groq API key for both nodes.

Verify Template Path

Ensure the Excel template is correctly referenced in the n8n workflow.

1. In n8n, click on the "Load Template" node
2. Verify the "File(s) Selector" field shows:

/templates/CIS_RAM_v2_1_for_IG1_Workbook_22_05_TEST.xlsx

3. This path should already be correct if the template is in the templates folder as specified in section

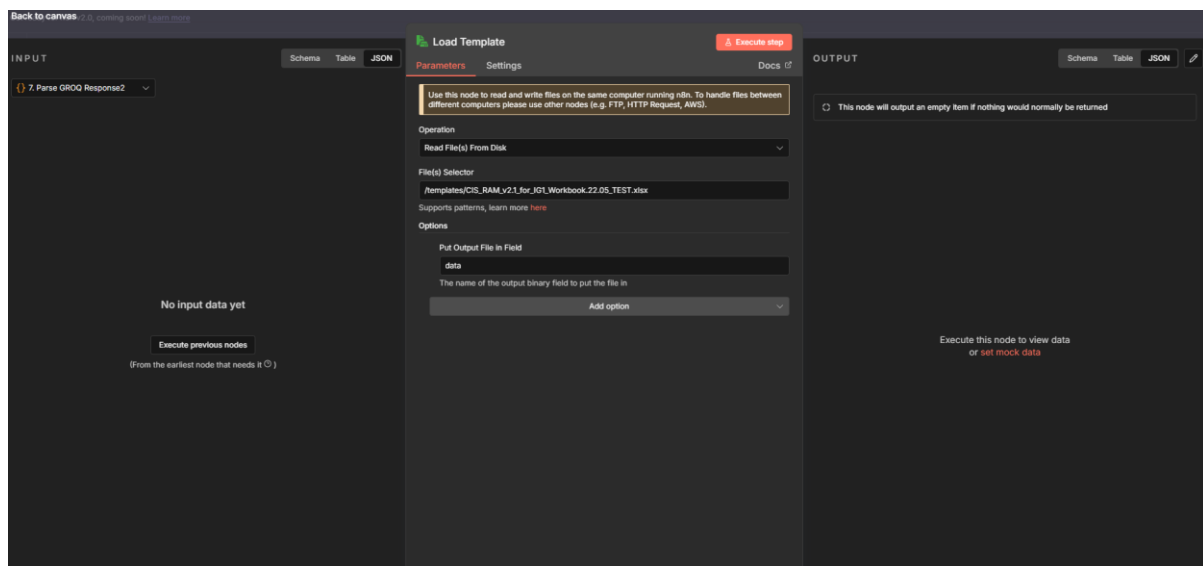


Figure 7: Load Template node showing correct file path configuration

Configure Email Credentials (Optional)

If you want the system to email completed reports, you must configure SMTP credentials. If you skip this step, the system will still function but will not send email reports. You can download the final excel from the node before Send email.

1. In n8n, click on the "Send email" node
2. Click the "Select Credential" dropdown at the top of the parameters panel
3. Click "+ Create New Credential"
4. Fill in your SMTP details:
 - User: Your email address
 - Password: Your email password or app-specific password
 - Host: Your SMTP server (e.g., smtp.gmail.com)
 - Port: Typically 465 (SSL) or 587 (TLS)
 - SSL/TLS: Enable for secure connection
5. Click "Save"
6. Select your newly created credential from the dropdown

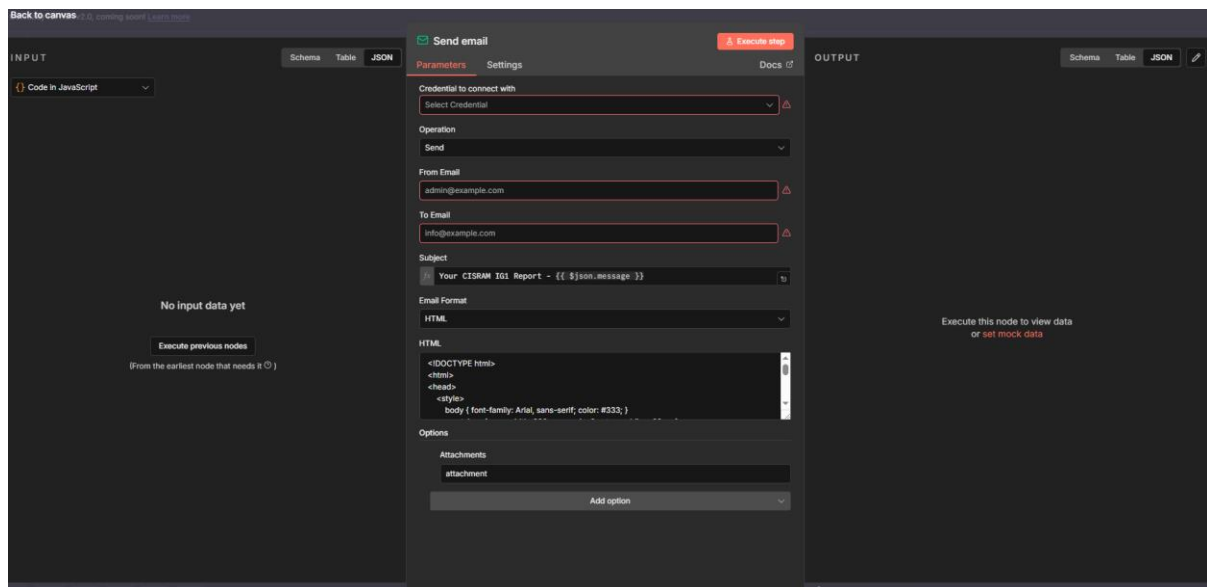


Figure 8: Send email node showing credential selector

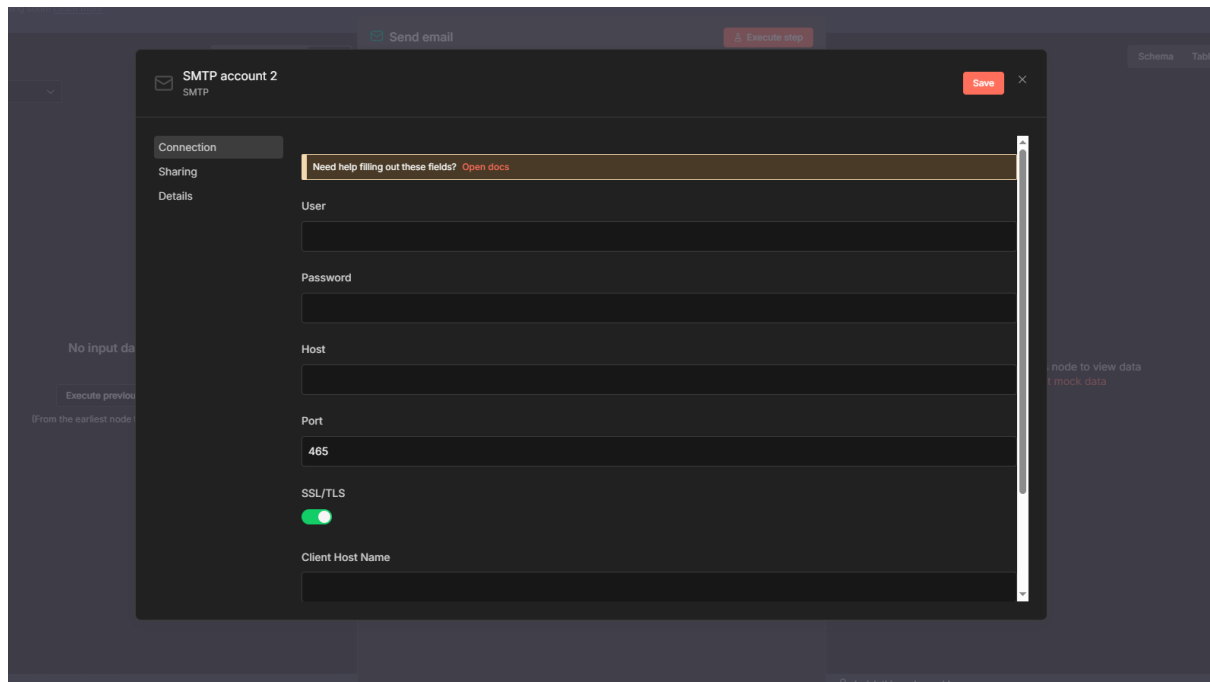


Figure 9: SMTP credential configuration dialog showing required fields

Note: Gmail users may need to create an "App Password" rather than using their regular password. See <https://support.google.com/accounts/answer/185833> for instructions.

8. Start React Application

1. Open new Command Prompt window
2. Navigate to React application directory
3. Install dependencies (first time only):

npm install

4. Start development server:

npm run dev

5. Note displayed URL (typically <http://localhost:5173>)
6. Open the URL in your web browser
7. Grant microphone permissions when prompted

The system is now ready to conduct voice-based cybersecurity assessments.

9. Key System Parameters

System behaviour parameters are configurable in the main React component file (src/App.jsx):

Parameter	Value	Purpose
WHISPER_CHUNK_INTERVAL	3000ms	How often audio is sent to Groq Whisper
DEAD_AIR_HIDDEN_PERIOD	5000ms	Silent countdown before visible timer
DEAD_AIR_COUNTDOWN_PERIOD	5000ms	Visible countdown duration
MIN_TIME_BETWEEN_CALLS	5000ms	Minimum time between Groq API calls (rate limiting)
MIN_WORDS_FOR_CONTENT	3 words	Threshold for detecting filler words
MIN_SPEECH_LEVEL	15	Audio level threshold for speech detection
Groq Model Options	gpt-oss-120b gpt-oss-20b	120b: Best 20b: Cheapest

Table 2: System Parameters

10. Stopping the System

Stop React Application

Press Ctrl+C in Command Prompt where React application is running.

Stop n8n Container

Navigate to directory containing docker-compose.yml and run:

docker-compose down

11. Troubleshooting

Issue: n8n container won't start?

Solution: Ensure Docker Desktop is running. Check that port 5678 is not already in use by another application.

Issue: React application can't connect to n8n?

Solution: Verify n8n is running at http://localhost:5678 and the workflow is activated.

Issue: Microphone not working

Solution: Check browser permissions. The browser must be granted microphone access when prompted.

Issue: Groq API errors

Solution: Verify API keys are correctly entered in both the .env file and the two n8n Groq nodes. Ensure the API key has not exceeded usage limits.

Issue: Email not sending

Solution: Verify SMTP credentials are correct. Check that the email provider allows SMTP access (Gmail requires App Passwords).