Snort MCP (Model Context Protocol) – Latest

Snort MCP is an AI-assisted security analysis project that integrates **Snort IDS** with **Model Context Protocol (MCP)** and **Groq LLM APIs** to provide intelligent insights from intrusion detection logs.

This repository is designed for **local or server-based deployment** with a simple and secure setup process.

Features

- Snort Intrusion Detection integration
- AI-powered log and alert analysis
- MCP-based contextual processing
- Groq LLM support
- Secure API key handling via environment variables

Prerequisites

Ensure the following are installed on the system:

- Python **3.9 or above**
- Snort (installed and configured)
- Git
- A valid **Groq API Key**

Important: Groq API Key

⚠ **The `GROQ_API_KEY` is not included in the repository.**

You must **share the API key manually** with the client.
The client will set it locally as an environment variable.

Setup Guide (For Clients)

Step 1: Clone the Repository

```
git clone https://github.com/Sardarmani/SnortMCPLatest.git
cd SnortMCPLatest
```

Step 2: Create a Virtual Environment (Recommended)

```
python3 -m venv venv
source venv/bin/activate
```

Windows:

```
venv\Scripts\activate
```

Step 3: Install Dependencies

```
pip install -r requirements.txt
```

Step 4: Set Groq API Key (Manual)

Linux / macOS

```
export GROQ_API_KEY="your_api_key_here"
```

Windows (PowerShell)

```
setx GROQ_API_KEY "your_api_key_here"
```

Restart the terminal after setting the key.

Step 5: Verify API Key

```
echo $GROQ_API_KEY
```

Windows:

```
echo $env:GROQ_API_KEY
```

Step 6: Run the Application

```
python main.py
```

(If the entry file name differs, adjust accordingly.)

How It Works

1. Snort generates alerts and logs
2. MCP processes Snort data
3. Groq LLM analyzes the context
4. AI-generated insights are produced

Project Structure

```
SnortMCPLatest/
│
├── main.py
├── requirements.txt
├── snort/
├── mcp/
├── utils/
└── README.md
```

Troubleshooting

GROQ_API_KEY not detected

- Ensure it is set correctly
- Restart the terminal
- Verify using `echo`

Snort not working

- Confirm Snort installation
- Check Snort configuration paths

Support

For setup assistance or customization, contact the repository maintainer.

License

This project is intended for internal, educational, or research use.