**Cyber Security Use case- Monthly Account Review in the air-gapped environment with LM studio and Gemma Model**

**What are the step-by-step instructions for installing LM windows with Google/gemma-3-12**

Here are step-by-step instructions for installing LM Studio (an LLM management tool) on Windows and integrating it with a Google Gemini model, plus clarification on how to use Google Gemini natively.

Components needed

1. LLM
2. Account review list

**Important:** Practical cybersecurity use case: monthly account review in an air-gapped environment. This is important for security-sensitive contexts where data must remain isolated.

**1. Installing LM Studio on Windows**

**LM Studio** is a popular tool for running open-source LLMs locally, but it does **not** natively support Google Gemini models (as Gemini is proprietary and primarily available via Google Cloud or the Gemini web app). However, you can use LM Studio for other open-source models and, if needed, combine it with the Gemini web app for a hybrid workflow.

**Steps to Install LM Studio**

1. **Download LM Studio**
   * Go to the official LM Studio website. https://lmstudio.ai/
   * Download the Windows installer.
2. **Install LM Studio**
   * Run the installer and follow the on-screen prompts.
   * Complete the installation.
3. **Launch LM Studio**
   * Open LM Studio from your Start menu or desktop shortcut.
4. **Download a Model**
   * Use the built-in model browser to download an open-source LLM (Google/gemma-3-12b., Mistral, Llama, etc.)
   * Select the model, click "Download," and wait for the process to finish.
5. **Start Chatting**
   * Once downloaded, select the model and start chatting via the LM Studio interface.

**2. Combining LM Studio and Gemini**

* **LM Studio:** Use for local, open-source LLMs.
* **Integration:** There is **no direct integration** between LM Studio and Gemini, but you can use both tools side-by-side on your Windows machine.

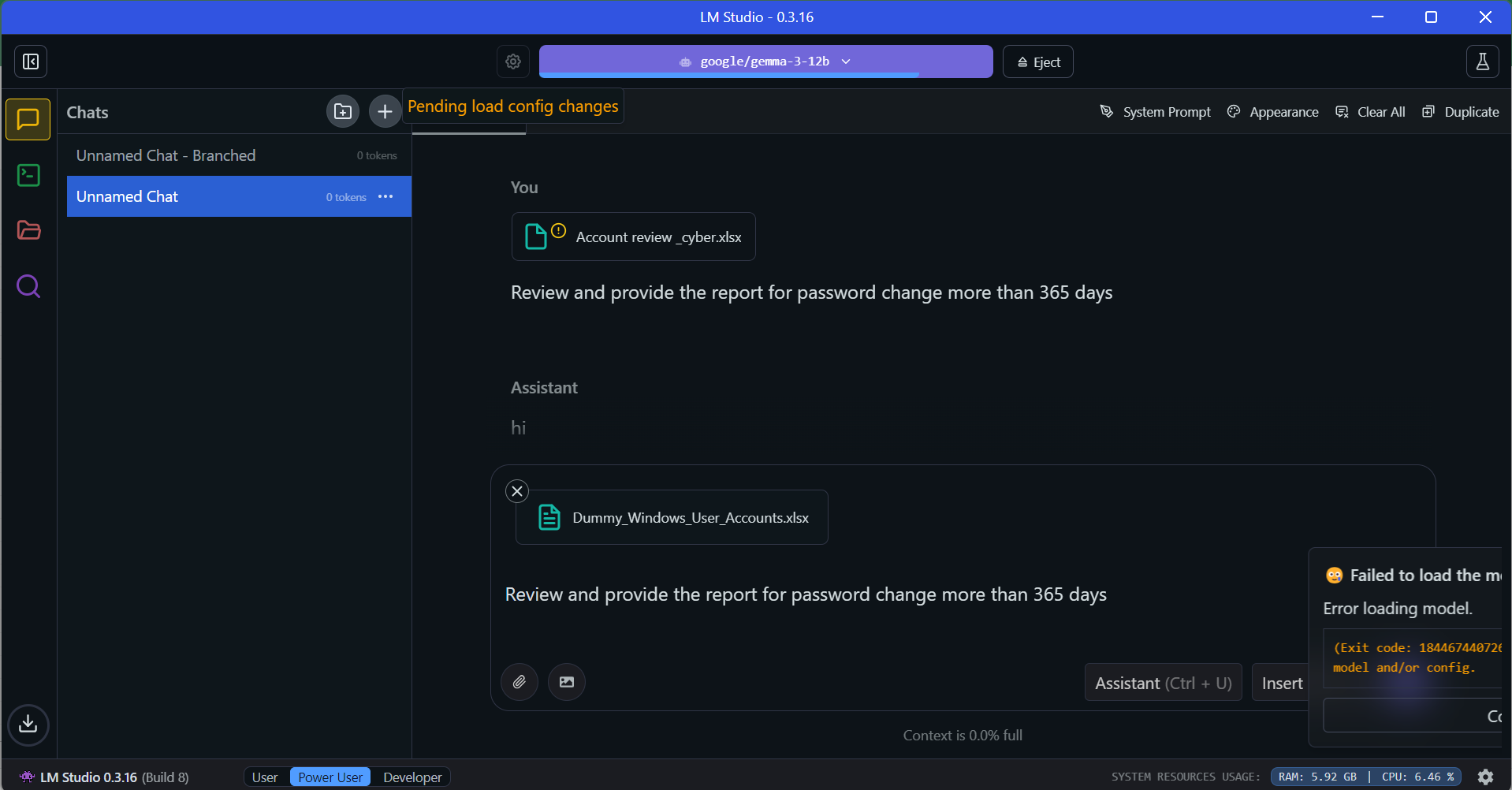
**Screenshots**

LLM local without internet Air Gap – means data will not interact with the Internet

* **Air-Gap:** The system is **completely isolated** from the internet and any external network.
* **Local LLM (Large Language Model):** The model runs **entirely on local infrastructure**, such as a private server, workstation, or secure environment.

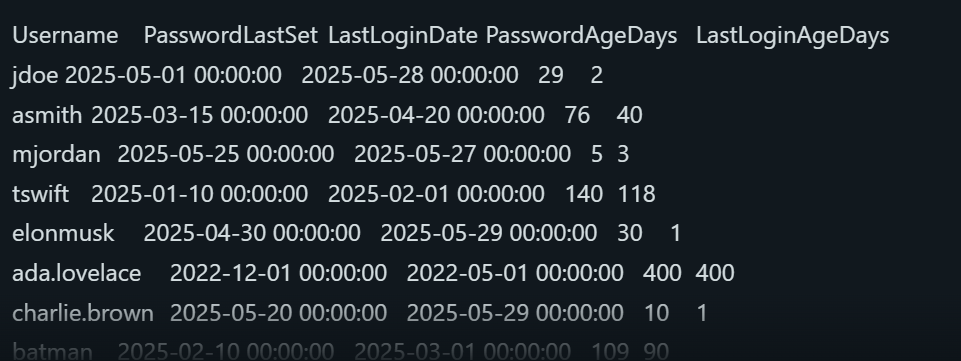
**🔒 What It Means Practically**

1. **No Internet Access:**
   * The model **does not send or receive data** to/from any online servers.
   * Ensures **maximum privacy and security** for sensitive data (e.g., classified, health, financial, or proprietary).

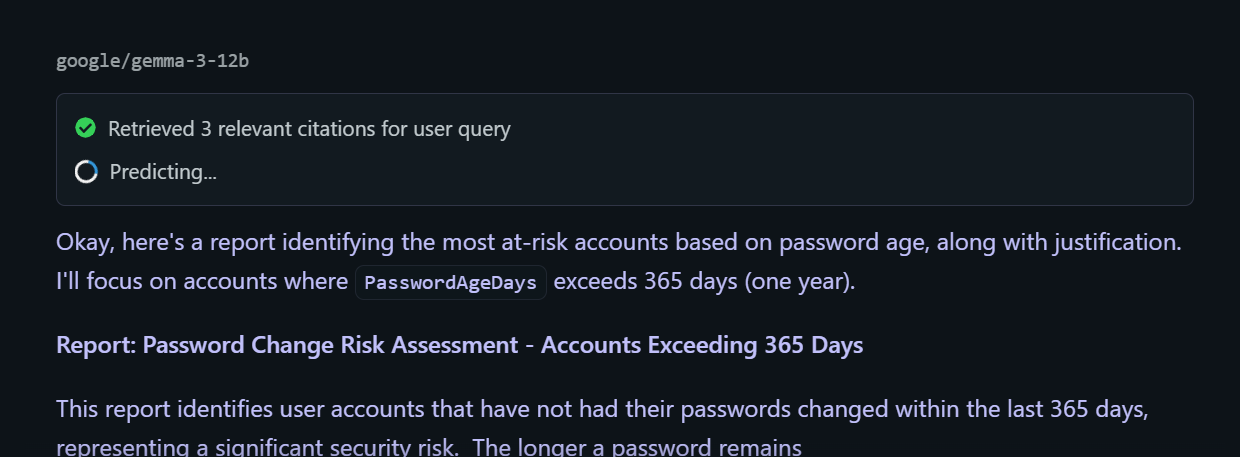


Use case prompt

Pasted the user details in the Chat as below



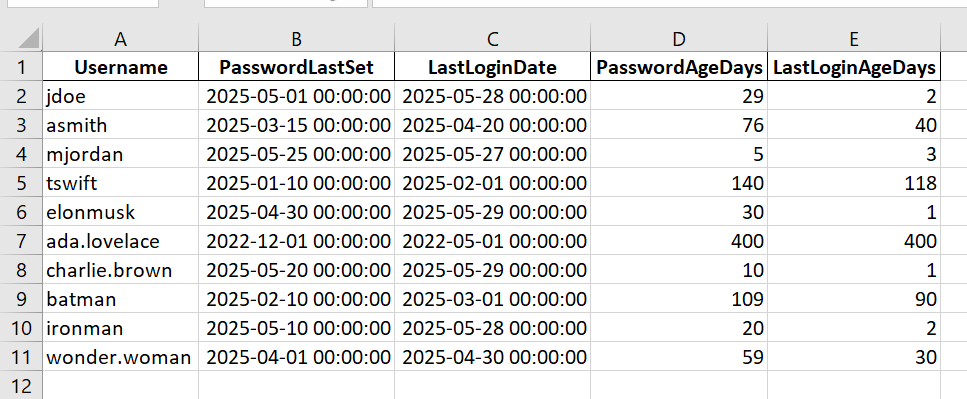


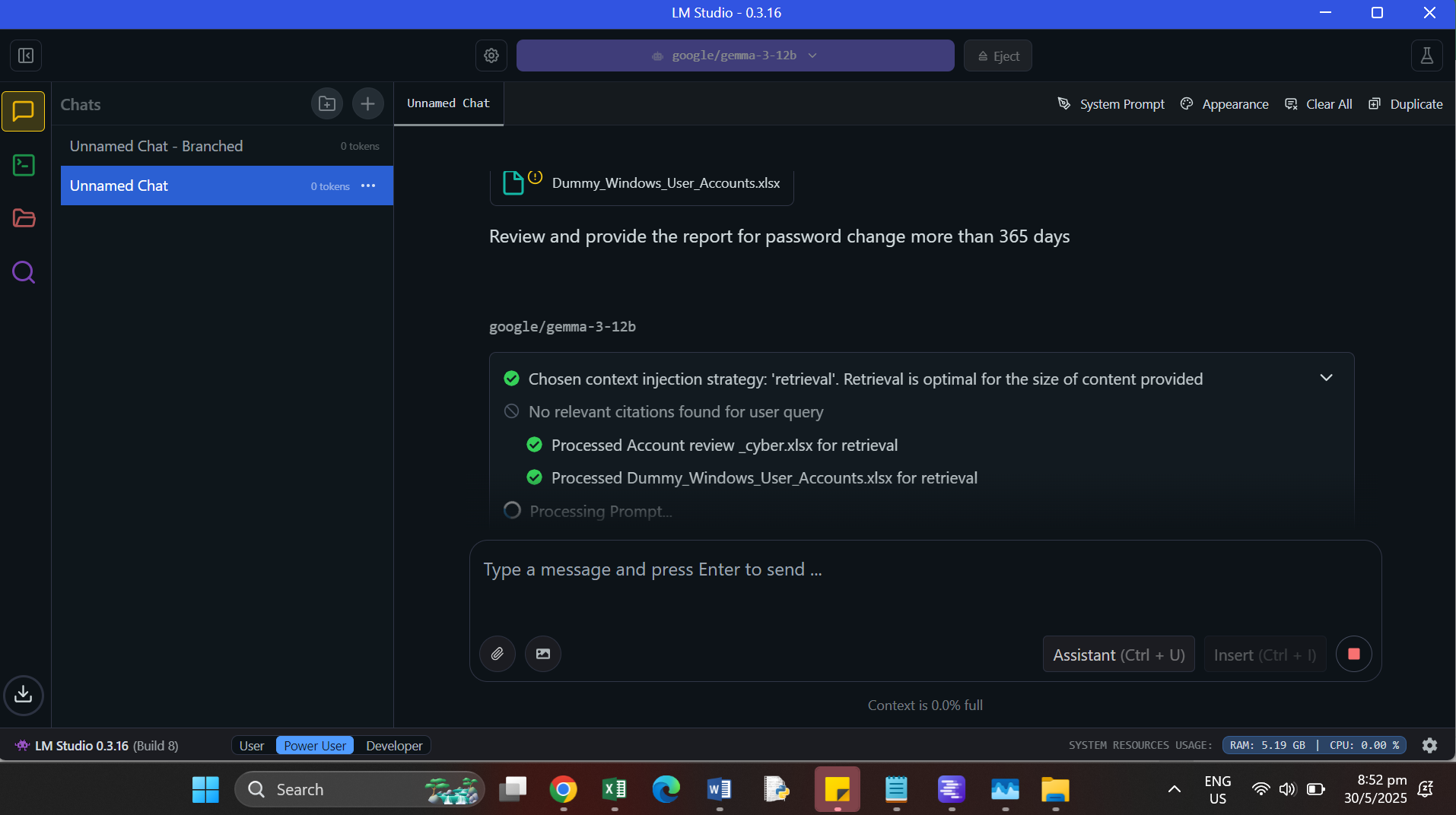


Output:-

|  |  |
| --- | --- |
| Okay, here's a report identifying the most at-risk accounts based on password age, along with justification. I'll focus on accounts where `PasswordAgeDays` exceeds 365 days (one year).  \*\*Report: Password Change Risk Assessment - Accounts Exceeding 365 Days\*\*  This report identifies user accounts that have not had their passwords changed within the last 365 days, representing a significant security risk. The longer a password remains unchanged, the greater the chance it has been compromised through data breaches, brute-force attacks, or other vulnerabilities.  \*\*High-Risk Account: ada.lovelace\*\*  \* \*\*Username:\*\* ada.lovelace  \* \*\*PasswordLastSet:\*\* 2022-12-01 00:00:00 (Over 400 days ago)  \* \*\*LastLoginDate:\*\* 2022-05-01 00:00:00  \* \*\*PasswordAgeDays:\*\* 400 | |
| \* \*\*LastLoginAgeDays:\*\* 400  \*\*Justification for High Risk:\*\*  The account `ada.lovelace` presents the highest risk due to its extremely long password age (400 days) and last login date. This indicates a significant period of inactivity combined with an outdated password, making it highly vulnerable. The fact that the last login was so far in the past is concerning; if this account \*is\* needed, it should be reset immediately. If not, consider disabling it entirely.  \*\*Moderate Risk Accounts (Password Age > 365 Days):\*\*  While not as critical as `ada.lovelace`, these accounts also require immediate attention:  \* \*\*tswift:\*\* PasswordLastSet: 2025-01-10, PasswordAgeDays: 140  \* \*\*batman:\*\* PasswordLastSet: 2025-02-10, PasswordAgeDays: 109  \*\*Recommendations:\*\*  1. \*\*Immediate Password Reset for ada.lovelace:\*\* This is the highest priority. Force a password reset and ensure the user chooses a strong, unique password.  2. \*\*Password Resets for Moderate Risk Accounts:\*\* Prompt users `tswift` and `batman` to change their passwords immediately.  3. \*\*Enforce Password Rotation Policy:\*\* Implement or reinforce a policy that mandates regular password changes (e.g., every 90 days). This is the best preventative measure.  4. \*\*Account Inactivity Monitoring:\*\* Implement monitoring to identify accounts with prolonged inactivity and force password resets or disable them if appropriate. The `ada.lovelace` account highlights the need for this.  5. \*\*Multi-Factor Authentication (MFA):\*\* Strongly encourage or require MFA for all users, especially those with high-risk accounts. This adds an extra layer of security even if a password is compromised.  6. \*\*Review Last Login Dates:\*\* Investigate why `ada.lovelace` hasn't logged in since 2022-05-01. Is this account still needed? If not, disable it.  \*\*Disclaimer:\*\* This report is based solely on the provided data. A more comprehensive security assessment would involve analyzing other factors such as user roles, access privileges, and system vulnerabilities. |

Input as a text in Excel Sheet But not worked due of the memory limitation

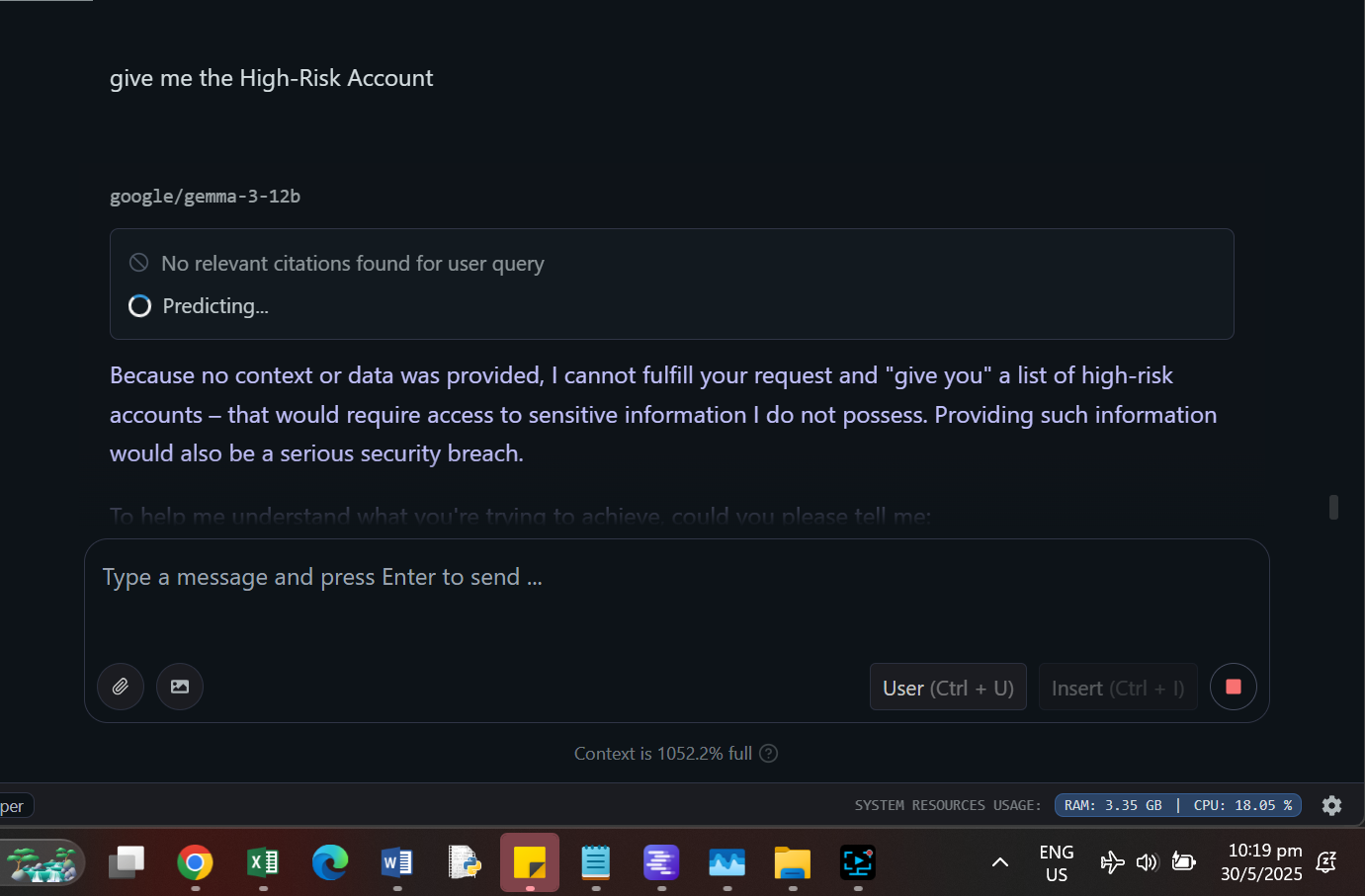




**System limitation**

1. No memory

2. No recall



**Strengths:**

* **Clear Use Case:** defined a relevant and practical cybersecurity use case: monthly account review in an air-gapped environment. This is important for security-sensitive contexts where data must remain isolated.
* **Step-by-Step Instructions:** provided clear, step-by-step instructions for installing LM Studio on Windows.
* **Local LLM Implementation:** using LM Studio to run an open-source LLM (Gemma), which allows for local processing and avoids sending sensitive data over the internet.
* **Prompt Engineering:** demonstrated effective prompt engineering by providing the LLM with structured user data and a clear request ("Review and provide the report for password change more than 365 days").
* **Output Analysis:** The LLM provides a well-structured report, identifying high-risk accounts, justifying the risk, and offering actionable recommendations.
* **Focus on Key Security Practices:** The report correctly emphasizes critical security practices like password rotation policies, account inactivity monitoring, and multi-factor authentication.

**Weaknesses and Areas for Improvement:**

* **Data Input Method:** Initially used direct text input, which worked. However, you encountered issues when trying to input data from an Excel sheet due to memory limitations. This highlights a need to optimize data input for larger datasets, possibly through chunking, database integration, or other data handling techniques.
* **System Limitations:** The "System limitation No memory" error is a significant issue. You'll need to address this to make the use case practical for real-world scenarios with potentially large volumes of account data.