2. Database Creation (PostgreSQL)

The SOC Co-Pilot project utilizes PostgreSQL to store enriched security alerts processed by the Wazuh-AI pipeline. This section details the installation and configuration of the PostgreSQL database.

Installation

1. **Install PostgreSQL**:

   `bash sudo apt update sudo apt install postgresql postgresql-contrib -y`

Configuration

1. **Access PostgreSQL Shell**:

   Switch to the `postgres` user and launch the PostgreSQL shell:

   `bash sudo -i -u postgres psql`

2. **Create Database and User**:

   Inside the `psql` prompt, execute the following SQL commands:

   `sql CREATE DATABASE soc_copilot; CREATE USER soc_admin WITH PASSWORD 'spr888'; GRANT ALL PRIVILEGES ON DATABASE soc_copilot TO soc_admin;`

   Note: Ensure the `CREATE USER` command completes successfully before proceeding. If you encounter an error like "role `soc_admin` does not exist" when trying to `ALTER USER`, it indicates the user was not created. Re-run the `CREATE USER` command.

3. **Exit PostgreSQL Shell**:

   `sql \q`

[Reference: `NOTES(1).pdf`]