**📊 XDR System Monitoring Project**

**📁 Project Overview**

**This project is an Extended Detection and Response (XDR) Agent + Server System, built with Python and Flask. It collects system and process-level metrics from multiple clients machines and stores the data in MySQL databases, one per agent. Data is then available for visualization (e.g., Power BI).**

**🔧 Project Components**

**🖥️ Agent Script (Client Side)**

* **Collects system metrics: memory, CPU, disk, network I/O.**
* **Collects process metrics: PID, name, username, memory/CPU usage, open files, command line, and flags suspicious file types.**
* **Sends data to the server every 60 seconds.**

**🌐 Flask Server (Backend)**

* **Receives incoming JSON data via /ingest endpoint.**
* **Validates authorization token.**
* **Dynamically creates a dedicated MySQL database per hostname/agent.**
* **Stores metrics into two tables:**
  + **system\_metrics**
  + **process\_metrics**

**📂 Folder Structure**

**xdr\_project/**

**├── xdr.ipynb # Agent-side script (client)**

**├── server.ipynb # Flask server that receives and stores data**

**└── Final Craw Project # Power-bi file**

**⚙️ Setup Instructions**

1. **install Requirements**

**Make sure to install required libraries on both server and agent systems:**

**pip install flask mysql-connector-python psutil requests**

1. **Update Server IP and Token**

**In agent.py, change these lines to match your setup:**

**SERVER\_URL = "http://<your-server-ip>:5000/ingest"**

**AUTH\_TOKEN = "psg\_xdr\_agent\_token"**

1. **Configure MySQL Credentials**

**In server.py, update the db\_config dictionary:**

**db\_config = {**

**'host': 'localhost', # Use actual MySQL server IP if remote**

**'user': 'your\_mysql\_user',**

**'password': 'your\_mysql\_password',**

**}**

**4️. Start the Server**

**python server.py**

**5️. Run the Agent**

**Run this on each client machine:**

**python agent.py**

**🧪 Output**

* **Each system sends data every 60 seconds.**
* **MySQL creates a new database like my-laptop\_db for each hostname.**
* **Data is stored in system\_metrics and process\_metrics.**

**📊 Next Step: Power BI Integration**

* **Use MySQL connector in Power BI.**
* **Connect to each agent's DB for dashboards.**

**👨‍💻 Author**

* **Abhinav Singh**
* **GitHub:** [**hhttps://github.com/AbhinavSuryavanshi**](hhttps://github.com/AbhinavSuryavanshi)
* **LinkedIn:** [**www.linkedin.com/in/abhinav-singh-607760213**](www.linkedin.com/in/abhinav-singh-607760213)
* **Email: Suryavanshiabhinav206@gmail.com**