Objective:

Develop an AI-based multi-agent system that can detect, prevent, and respond to cybersecurity threats within an organization. The system should simulate various attack scenarios, defense mechanisms, and response strategies.

---

1. Input Data Details

Primary Data:

- **Network Traffic Data:** Logs capturing network flows, packet details, and anomalies.
- **System Event Logs:** OS logs, application logs, and security logs indicating suspicious activities.
- **Threat Intelligence Feeds:** Indicators of compromise (IOCs), known attack signatures, and vulnerability data.
- **User Behavior Data:** Login patterns, access logs, and behavioral anomalies.
- **Configuration Data:** System and network configurations, patch levels, and security policies.

Preparation Tips:

- Use simulated or anonymized logs to mimic real-world attack and defense scenarios.
- Label data with attack types, threat levels, or anomalies for supervised learning.

---

2. Expected Outputs

Primary Goals:

- **Threat Detection:**
    - Input: Network/system logs and threat intelligence.
    - Output: Alerts or labels indicating potential threats or anomalies.
- **Automated Response Strategies:**
    - Recommendations or automated actions such as isolating systems, blocking IPs, or initiating scans.
- **Adaptive Learning:**
    - The system should improve over time by learning from new threats and responses.

Additional Outputs:

- Visual dashboards showing threat levels, attack vectors, and response status.

- Reports summarizing incidents and system health.

---

3. Key Requirements & Guidelines

- **Data Handling:**
    - Use labeled datasets for supervised learning where possible.
    - Incorporate unsupervised anomaly detection for unknown threats.
- **Modeling Approaches:**
    - Use multi-agent architectures with specialized agents for detection, response, and learning.
    - Techniques: Deep learning (e.g., LSTM, CNN), anomaly detection, reinforcement learning.
- **Features to Consider:**
    - Network flow features (source/destination IPs, ports, packet sizes).
    - System event features (login times, failed attempts, privilege escalations).
    - Threat intelligence indicators.
    - Behavioral patterns.
- **Evaluation Metrics:**
    - Detection accuracy, precision, recall.
    - Response effectiveness (e.g., time to contain threats).
    - False positive/negative rates.
- **Deliverables:**
    - Prototype multi-agent system with code/scripts.
    - Demonstration of threat detection and response.
    - Documentation explaining architecture, data used, and results.

---

4. Additional Datasets & Resources Needed

- **Simulated Network Traffic & Logs:** For attack and normal behavior.
- **Threat Intelligence Data:** Sample IOC feeds or simulated threat signatures.
- **Vulnerability Data:** Common vulnerabilities and exposures (CVEs).

- **Behavioral Data:** Simulated user activity logs.