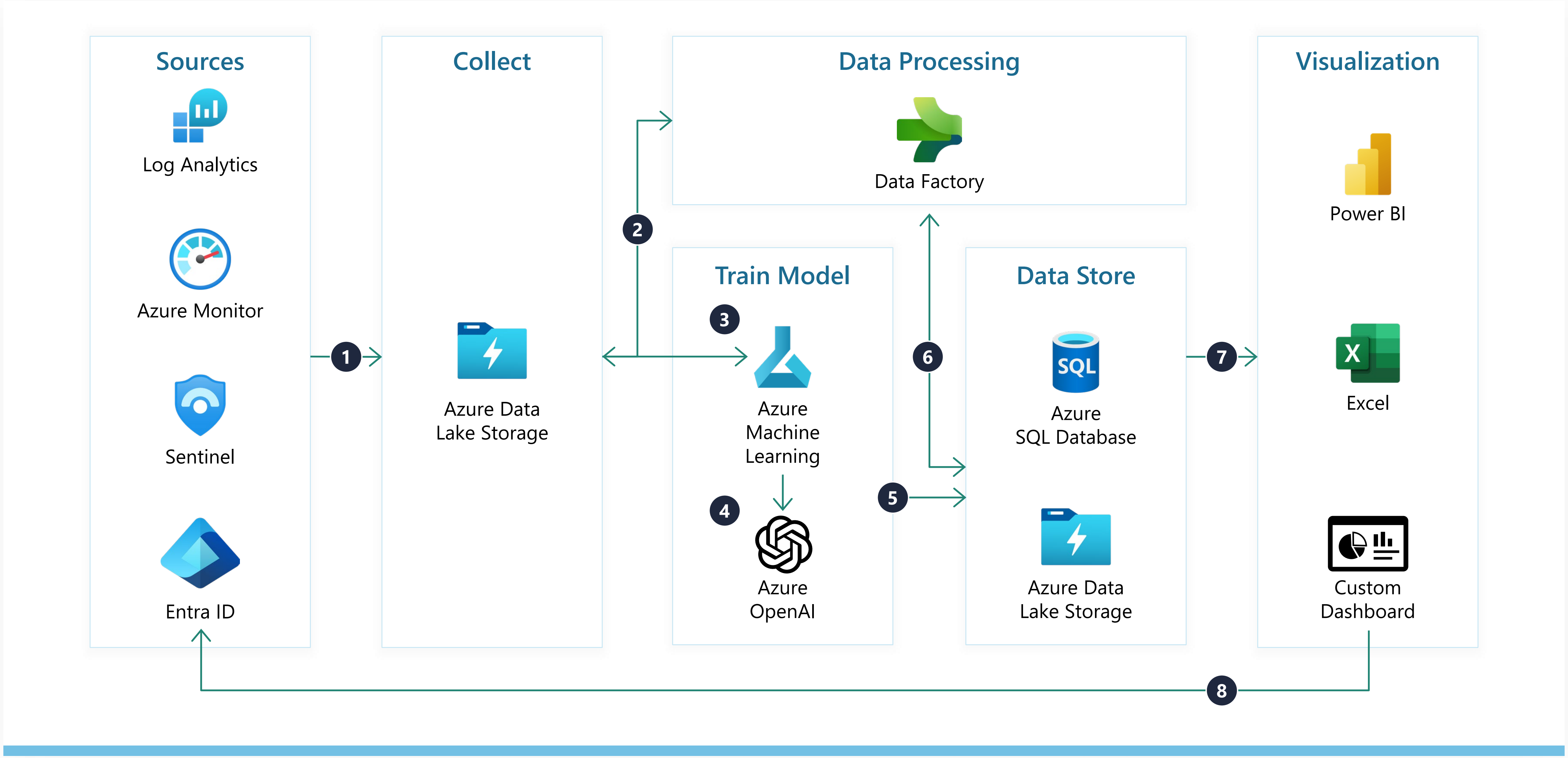
Cybersecurity

Cybersecurity Reference Architecture



Cybersecurity Reference Architecture

1 **Authentication and User Behavior Data Collection:** This step involves gathering data related to user authentication and behavior from Azure Active Directory (AD). The data includes login times, user locations, device types, and other authentication-related information.

The collected data is then securely stored in Azure Data Lake storage. It's crucial that the data is organized effectively to facilitate efficient analysis.

2 **Data Preprocessing:** Before analysis, the data is preprocessed and normalized using Azure Data Factory. This process ensures the data is in a suitable format for machine learning.

3 **Machine Learning Model Training:** Azure Machine Learning is employed to train models on the user behavior data. These models are designed to identify and learn normal behavior patterns for each user.

4 **Integration with Azure OpenAI:** Azure OpenAI Service is used to enhance the analysis, particularly in recognizing complex patterns and generating predictive models. These models are capable of detecting subtle behavioral anomalies that might indicate security risks.

5 Upon detecting an anomaly by Azure Machine Learning and Azure OpenAI models, record the anomaly incident and any recommended or taken actions in a database or data store within Azure SQL Database or Data Lake Storage. Store relevant details such as the nature of the anomaly, associated risk level, generated security recommendations, and actions taken
(e.g., type of MFA implemented).

Cybersecurity Reference Architecture

6 Use Azure Data Factory to process and enrich the recorded data, which may include data aggregation, classification by risk level, and summarization of incidents.

7 Integration with Visualization Tools: Connect the database or data store with data visualization and analysis tools like Microsoft Power BI or Excel. Interactive dashboard in Power BI or a report in Excel that displays key metrics such as the number of security incidents, types of detected anomalies, and the effectiveness of MFA recommendations.

8 Dynamic MFA Adjustment: Depending on the risk level assessed by the AI models, the MFA requirements are adjusted in real time. This could range from requesting additional authentication factors for minor anomalies to more stringent measures like biometric verification for higher risks. In extreme cases, user accounts might be temporarily locked, requiring direct intervention from the security team.