Answer sheet

QUESTION-1: Give a visualization scheme

ANSWER:

According to the meaning of the question, it is necessary to discover and classify the internal assets of the enterprise, and give the communication mode between the assets.

1. Our algorithm needs to mine log data, find out the classification behind the data, and display the results of asset discovery and classification.

2. The results of classification are presented relationally. In order to query the information of data flow conveniently, it is necessary to display the information of nodes interactively.

3. We need to find out the communication mode between assets. We use protocol and port information to discover and visualize the communication mode according to the classification results and the communication relationship of assets.

4. In order to facilitate the company to monitor the data traffic on that day, we display the upstream bandwidth and downstream bandwidth. In addition, according to the bandwidth usage, we can facilitate the company to adjust the network bandwidth usage.

5. We increase the display of machine activity to facilitate the monitoring of machine activity in different time periods. Prevent aggression during inactive periods.

QUESTION-2: Identify and classify assets within an enterprise

ANSWER:

According to the requirements, on the one hand, we need to discover the assets inside the enterprise, on the other hand, we need to classify the assets inside the enterprise.

1. Discovery of assets within an enterprise

* We use the relationship between nodes to construct the network, and process the edge attributes into the weight of the network to represent the network.

* The node2vec algorithm is used to vectorize the representation structure, and the TSNE algorithm is used to reduce the dimension of the observation data for partitioning.

* KMEANS algorithm is used to classify the data, and the category with the least loss is selected as the result of asset discovery.

2. Classification of enterprise assets

* We use clustering algorithm to classify the types of assets found, and label the corresponding types for each data.

QUESTION-3: Give the communication mode between assets

ANSWER:

According to the requirements, we can know that different protocols and ports are used for communication according to the asset classification in the figure.

1. We add filtering function to display the communication machine relationship in this mode according to the communication mode of port and protocol combination.

2. Provide interactive function, trigger the relationship between the sides, can update the left side of the IP communication diagram, and display IP-related node information. Mouse hover can view ports, upstream and downstream traffic, communication protocols.

QUESTION-4: Increasing Bandwidth Display Function and Visualizing Active Machines at Different Times in 24 Hours

ANSWER:

Real-world networks often encounter network attacks

1. We add the upstream traffic statistics and downstream traffic statistics on the same day to facilitate the monitoring of traffic anomalies.

2. We display the number of active machines in 24 hours to monitor the abnormal activity.