asma

know your assets

Increase Your Security Level By Ensuring Network Visibility

About ASMA

ASMA is a web based cyber security software developed to detect your network assets and manage them. It discovers the MAC and IP addresses of the assets, operating systems, and running services and helps you to maintain the information such as the owner, responsible, brand, model.

- First target of attackers are the unknown systems. Unknown systems have weaknesses because they cannot be updated since they are not managed.
- Organizations are not aware of unauthorized assets on their networks.
- Unauthorized changes on the systems cannot be detected.
- Since asset inventory applications are not security oriented, they cannot detect unauthorized assets newly joined the network.

- Detecting assets on the network with active and passive discovery methods is necessary and so is the owner, responsible and priority of the assets.
- It is important to detect the assets without owner or responsible.
- Up to date inventories will increase the network visibility.
- Anomalies can be detected by ensuring network visibility.

ACTIVE, PASSIVE ASSET DETECTION

NEW SERVICE DETECTION

NEW ASSET DETECTION

SERVICE CHANGE DETECTION

How It Works

ASMA basically consists of two components: management server and sensor.

Sensor component is a hardened virtual server installed on the network segment on which assets and services will be discovered. By performing continuous passive listening and active discovery on the relevant network segment, the sensor discovers the assets and the running services.

Management server is, on the other hand, used to collect the data from sensors, manage asset inventory, to observe alarms and warnings and to report. Management server is a hardened virtual server that can be installed on any segment of the network.

What is Active Scanning?

Active scanning is a method used to detect the TCP services on the assets with IP addresses. The aim with active scanning is to discover the TCP services on OSI 4th layer. During active discovery, the sensor interacts with the service running on the relevant asset, so it is affected by the protection methods such as FW installed on asset. Scanning is performed on well-known TCP ports during discovery. Since the sensor is located on the same network segment with the assets, the scanning does not go out of the relevant network segment.

What is Passive Scanning?

Passive scanning is a discovery method operated on OSI 2nd layer and used to discover the assets with IP addresses. During passive scanning, the sensor listens to the ARP/RARP packages produced by assets on the network segment it is located and provides asset discovery. The sensor does not interact any assets during passive listening.

IPv4 ADDRESS CHANGE DETECTION

MAC ADDRESS CHANGE DETECTION

ASSET BASED CORRELATIVE ANOMALY DETECTION

EASY ASSET MANAGEMENT WITH USER FRIENDLY INTERFACE

BARiKAT

▸ Cyber Security

KNOW YOUR NETWORK

Barikat B.V. Millenium Tower
Floor 29, Radarweg 29,
1045 XN
Amsterdam,
NETHERLANS

barikatbv.com

+ 31 20 854 61 46