KPI(Key Performance Indicator) de detección de una dirección MAC anómala:

Optamos por crear una base de datos con las MAC Asignadas por el IEEE(Institute of Electrical and Electronics Engineers) a los fabricantes más conocidos, también incluimos las MAC de la Empresa VMWare ya que crea dispositivos de conexión a redes virtuales, así como las MAC medianas y pequeñas que son un gran número de direcciones de distintos fabricantes, en total cubrimos 18562 direcciones MAC, de las aproximadamente 50373 registradas oficialmente.

Cuando la sonda detecta una conexión extraña, recogemos la MAC, tomamos los 3 primeros octetos y verificamos si aparece en la base de datos, entre los fabricantes más conocidos, en caso positivo, ya sabemos que la MAC de la conexión intrusa proviene de un dispositivo reconocido que usa MAC largas (de 3 octetos). En caso de no haber ninguna coincidencia, comprobamos los 3 primero octetos más el primer nibble del cuarto octeto con la tabla mac-m que contiene la lista de fabricantes de dispositivos de red que usan MAC medianas(3 octetos y medio y 20 bits de dispositivos = 1048576.), si no hubiera coincidencia comprobaríamos los 4 primeros octetos más el primer nibble del quinto octeto con la tabla mac-s que contiene las lista de fabricantes que usan MAC pequeñas(4 octetos y medio y 12 bit para dispositivos = 4096.), si no hubiera resultados en ningún caso, Consultaríamos a través de una API si la MAC pertenece a otro fabricante, hay múltiples opciones en línea, una de las web que nos parece mejor es: https://maclookup.app/, esta web ofrece la posibilidad de obtener una clave de la API (API key) muy útil para usar en una aplicación web, aunque también devuelve resultados en formato JSON usando el enlace: https://api.maclookup.app/v2/macs/, y agregando a continuación la MAC a investigar, esta web usa la versión 2 de la API, la última versión es la 3. Con todos estos filtros podemos decir que obtendríamos resultados casi al 100 %.

La base de datos hecha por nosotros no tiene datos de fechas, solo fabricante y dirección, la API de maclookup.app si muestra la fecha de actualización de la MAC del dispositivo y datos de si es privada.