**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 %.

Firewall con IDS & IPS

Dado que un firewall es un dispositivo de protección activo, se parece más a un sistema de prevención de intrusiones (IPS) que a un IDS (sistema de detección de intrusiones). Un IPS es como un IDS pero bloquea activamente las amenazas identificadas en lugar de simplemente levantar una alerta. Esto complementa la funcionalidad de un firewall, y muchos Firewall de última generación (NGFW) tienen funcionalidad IDS/IPS integrada. Esto les permite aplicar reglas de filtrado predefinidas (firewall) y detectar y responder a amenazas cibernéticas más sofisticadas (IDS/IPS).

Métricas de detección de intrusiones:

**Dispositivos no identificados en redes internas**

¿Cuál es el inventario de dispositivos autorizados en su red y cómo se mantiene y actualiza?

¿Cuántos activos hay en su red?

¿Cuántos de esos activos almacenan datos confidenciales?

¿Cuál es el proceso para responder a dispositivos no autorizados en la red y cómo se ponen en cuarentena y se monitorean estos dispositivos?

¿Cómo se protegen los dispositivos de IoT y cuál es el proceso para monitorear y parchear sus vulnerabilidades?

¿Cómo se implementa la segmentación de la red y cómo se segregan los diferentes tipos de dispositivos en la red?

¿Cómo se implementan los controles de acceso para los dispositivos de su red y cuál es el proceso para otorgar y revocar permisos de acceso?

¿Cómo se autentican y autorizan los dispositivos antes de que se les permita conectarse a la red?

¿Cuál es la política para los empleados que traen sus propios dispositivos (BYOD) al trabajo y cómo se administran y protegen estos dispositivos?

¿Qué medidas existen para detectar y responder a puntos de acceso no autorizados u otra infraestructura de red no autorizada?

¿Cuál es el proceso para rastrear el ciclo de vida de los dispositivos en su red, incluida la adquisición, implementación, mantenimiento y retiro?

¿Cómo se integran de forma segura los dispositivos y servicios de terceros en su red y cuál es el proceso para administrar su acceso y permisos?

¿Cuál es la política de acceso remoto a su red y qué medidas existen para proteger y monitorear las conexiones remotas?

Intentos de intrusión:

¿Cuántos intentos de intrusión ha detectado y bloqueado su sistema de detección de intrusiones?

¿Cuál es el tiempo promedio que lleva investigar y responder a los intentos de intrusión detectados?

¿Cuál es el proceso para informar intentos de intrusión a las partes interesadas relevantes, incluida la administración, las autoridades legales y las fuerzas del orden?

¿Cuántos intentos de acceso no autorizados ha detectado y bloqueado su firewall?

¿Cuál es el proceso para investigar y responder a los intentos de intrusión detectados y cómo se comunican esos hallazgos?

¿Cómo se recopilan y analizan los registros y otros datos de eventos de seguridad, y qué herramientas y procesos se utilizan para este fin?

¿Cómo se clasifican y priorizan los incidentes de seguridad y qué procedimientos de respuesta existen para cada clasificación?

¿Con qué frecuencia se revisan los registros de seguridad y cuál es el proceso para revisarlos?

¿Cómo se correlacionan y analizan los eventos e incidentes de seguridad para identificar posibles amenazas y ataques?

¿Qué medidas existen para evitar falsos positivos y falsos negativos en los sistemas de detección de intrusos?

¿Cómo se monitorean los patrones y anomalías del tráfico de la red para detectar posibles intrusiones?

¿Cómo se actualizan y prueban los planes de respuesta a incidentes en respuesta a nuevos intentos de intrusión y tendencias de ataque?

¿Cómo se ajustan y afinan los controles de seguridad en función de los resultados de los esfuerzos de detección y respuesta a intrusiones?