PEC 4

> Diseño de plataformas de sensores y sus topologías, exponiendo sus características y la forma de diseñarlas.

Para diseñar una plataforma de sensores, tenemos que tener claros varios puntos importantes:

1. Definir amenazas
2. Cuantificar riesgos
3. Identificar recursos de información
4. Perfilar logs

Una vez hemos identificado los sitios donde vamos a poner los sensores, debemos averiguar que sensores queremos poner en cada sitio. Existen tres tipos de sensores:

- Collect only
- Half cycle
- Full cycle detection

Cada uno de ellos tiene sus ventajas e inconvenientes, pero el mas común, es el Half cycle, porque puede interceptar el trafico, ademas de realizar tareas de detección.

Una vez tengamos estos datos, debemos pensar donde vamos a colocar los distintos sensores. Para obtener el mejor resultado, debemos hablar con el equipo de redes, para que nos proporcionen esquemas simplificados de la red interna.

Idealmente, debemos poner un sensor en cada punto de entrada o salida de paquetes de nuestra red, de esta forma, vamos a tener la oportunidad de interceptar cualquier malware que haya entrado en la red, o que este intentando conectar con el servidor de C&C.

Si la red es demasiado grande y el trafico que pasa por los puntos de entrada salida de la misma es demasiado alto, debemos bajar en un nivel el sensor en la red.

Debemos poner el sensor lo mas cerca posible de los dispositivos críticos de la organización, para poder monitorizar correctamente. Por ejemplo, no es lo mismo un sensor que monitoriza el trafico desde fuera de la red interna, a un sensor que monitoriza el mismo trafico desde dentro de la red interna. Este segundo puede proporcionar mucha mas información que el primero.