PEC 3 - Diferencias entre las generaciones del SOC

- El SOC ha sido un trabajo de **desarrollo continuo durante los últimos 15 anos**.
- **4 generaciones incrementales**, de forma que cada generación construye sobre las bases de la generación anterior.

La evolución de las generaciones ha sido debida a los ataques, **cada vez mas sofisticados**.

Primera generación del SOC

Diferentes miembros del equipo técnico se centraban en gestionar los registros de los dispositivos que si que producían registros Estos registros se **almacenaban** y se revisaban únicamente cuando se había detectado alguna **incidencia**.

En el caso de alguna incidencia, el equipo que la gestionaba **trabajaba de forma desorganizada, no existía cadena de responsabilidades ni roles**. En resumen, es una gestión de la seguridad **pasiva y reaccionaria**.

Segunda generación del SOC

Aparece el concepto de **SIEM** Estas herramientas **analizaban la red en tiempo real** con el objetivo de detectar amenazas. Se **unificaban distintas fuentes de registros** para analizar posibles patrones maliciosos, que si identificadas, alertaban a los usuarios mediante una alerta en su **panel de control**.

Ademas, al tener una plataforma centralizada, se añadió la capacidad de **gestionar y asignar amenazas**.

Tercera generación del SOC

Existe una noción de **equipo del SOC**, que anteriormente, estaba distribuido entre los distintos miembros del equipo técnico. Se le añaden responsabilidades, como **gestión de vulnerabilidades** a las presupuestas de gestión de incidentes.

Cuarta generación del SOC

Expanden sobre la base ya existente de análisis de vulnerabilidades. Se centran en **analizar amenazas correlacionando datos de forma masiva** (Big Data) Ahora, incluso **distintas empresas pueden cooperar** para encontrar amenazas similares y anteponerse a la amenazas.

Enriquecimiento de datos, para obtener mas contexto en relación a los eventos que han ocurrido.

Despliegue de herramientas automatizadas de gestión de amenazas, como sistemas de prevención de intrusiones.

Se ha pasado a fase de **automatización y gestión de entornos as a code**.