**PROCEDIMIENTO DE ANALISIS ADMINISTRACION**

HISTORIA

HU6. Como responsable de administración necesito que se analicen los rastros de auditoría para hacer mejor seguimiento de actividades sospechosas

Criterio de aceptación: El nuevo Dashboard mostrará una gráfica con el seguimiento

TAREA

HU6-T2. Análisis exploratorio para analizar los rastros de auditoría para hacer mejor seguimiento de actividades sospechosas

**DESARROLLO**

El análisis exploratorio de los rastros de auditoría es un proceso esencial para detectar y hacer un seguimiento de actividades sospechosas en un sistema

**Recopilación de Datos de Auditoría**

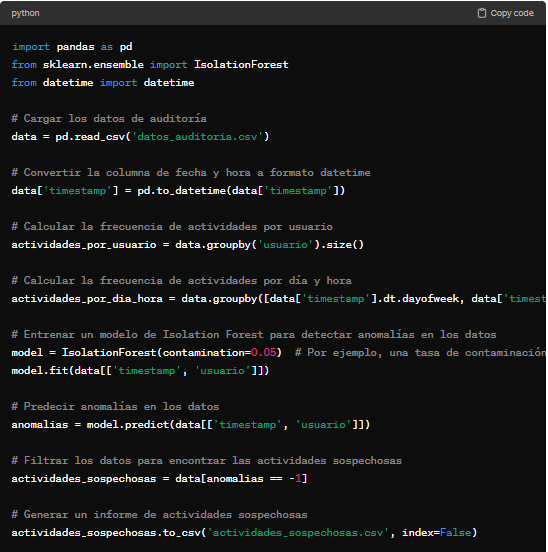
Limpieza y Preparación de Datos:

Se limpia y prepara los datos de auditoría para su análisis. Esto puede implicar la eliminación de datos incompletos o incorrectos, la estandarización de formatos, la conversión de datos en un formato adecuado para el análisis, etc.

**Exploración de Datos**

Realiza un análisis exploratorio de los datos de auditoría para familiarizarte con ellos y comprender su estructura y contenido.

Examina las diferentes variables disponibles en los datos de auditoría, como el usuario, la fecha y hora de la actividad, la acción realizada, el objeto afectado, etc.



* Se carga un conjunto de datos de auditoría desde un archivo CSV.
* Se convierte la columna de fecha y hora a formato datetime para facilitar su manipulación.
* Se calcula la frecuencia de actividades por usuario y por día/hora.
* Se entrena un modelo de Isolation Forest para detectar anomalías en los datos.
* Se utilizan las predicciones del modelo para identificar actividades sospechosas.
* Se genera un informe de actividades sospechosas que se guarda en un archivo CSV.

**Identificación de Patrones y Tendencias Normales**

Analizamos los datos para identificar patrones y tendencias normales en las actividades del sistema. Esto puede incluir la frecuencia y el horario de acceso de los usuarios, los tipos de acciones realizadas con mayor frecuencia, los objetos más afectados, etc.

**Detección de Anomalías**

Utilizamos técnicas de detección de anomalías, como análisis de series temporales, análisis de valores atípicos, o modelos de aprendizaje automático para identificar actividades sospechosas o inusuales en los datos de auditoría.

Buscamos actividades que se desvíen significativamente de los patrones y tendencias normales identificados en el paso anterior.

**Investigación de Actividades Sospechosas**

Una vez identificadas las actividades sospechosas, investiga más a fondo para comprender la naturaleza y el alcance de estas actividades.

Examina los detalles de las actividades sospechosas, como el usuario involucrado, la acción realizada, el objeto afectado, la fecha y hora de la actividad, etc.

**Generación de Informes y Alertas**

Creamos informes detallados sobre las actividades sospechosas detectadas, incluyendo información sobre la naturaleza de las actividades, los usuarios involucrados, las acciones realizadas y cualquier otro detalle relevante.

Configuramos alertas automáticas para notificar inmediatamente al personal de seguridad sobre actividades sospechosas en tiempo real.