Tu calificación: 86,66 %

Tu calificación más reciente: **86,66 %** • Tu calificación más alta: **86,66 %** • Para aprobar necesitas al menos un 80 %. Guardamos tu puntaje más alto.

Próximo artículo

Estás viendo una versión traducida automáticamente de esta evaluación
Puedes volver a ver el contenido en su idioma original si lo prefieres. No perderás el progreso que hayas conseguido si cambias el idioma. Mostrar la versión en Inglés

Introducción

Resumen de actividades

Como especialista en automatización de TI, estarás constantemente supervisando los sistemas en busca de anomalías y posibles amenazas a la seguridad. Las herramientas de IA generativa pueden ayudarle a automatizar tareas como el análisis de datos de inicio de sesión y la generación de alertas, liberando su tiempo para centrarse en iniciativas más estratégicas.

En esta actividad, utilizará una herramienta de IA generativa y el marco de instrucciones TCREI para escribir un mensaje a los usuarios. Esta actividad es opcional, pero la recomendamos para ayudarle a perfeccionar sus conocimientos sobre avisos. Si no puedes completar esta actividad, podrás seguir avanzando en el curso y obtener un certificado de Google.

Acceso a la herramienta Gen IA

Para completar esta actividad, puedes utilizar la herramienta de IA gen basada en navegador que prefieras. A continuación se ofrecen instrucciones para acceder a Gemini, que requiere una cuenta de Google.

Para acceder a Gemini

- Ve a gemini.google.com.
- Acceda a su cuenta de Google.

Consulta el recurso sobre cómo crear una cuenta de Google si aún no tienes una. Para obtener más ayuda sobre cómo acceder a Gemini, consulta la Ayuda de Gemini Apps.

- Para obtener más información sobre el uso de Gemini (por ejemplo, quién puede utilizar Gemini, el Aviso de privacidad de Gemini y dónde está disponible Gemini actualmente), consulta las FAQ de Gemini Apps.
- No introduzcas información privada o confidencial en tus conversaciones de Gemini, ni ningún dato que no quieras que Google utilice para mejorar sus productos, servicios y tecnologías de aprendizaje automático.

Detalles de la actividad

Paso 1: Introduzca su pregunta inicial

Paso 2: Evaluar el resultado inicial

Paso 3: Revisar y perfeccionar el mensaje

Paso 4: Evaluar de nuevo el resultado

Paso 5: Adoptar un enfoque iterativo

1. 1. ¿Qué partes del marco de orientación le resultaron más útiles? *Seleccione todas las que procedan.* **0.6 / 1 punto**

- [x] Tarea (incluyendo persona y formato)
  - Correcto
- [x] Contexto
  - Correcto
- [x] Referencias
  - Correcto
- [ ] Evaluación
- [ ] Iterativo

No seleccionaste todas las respuestas correctas

2. 2. Presente la sugerencia que considere que mejor satisface su objetivo y que proporciona suficiente especificidad, contexto y referencias pertinentes para producir un resultado útil y eficaz. **1 / 1 punto**

El objetivo principal es supervisar la actividad de inicio de sesión del usuario, identificar patrones sospechosos y generar alertas cuando el comportamiento se desvía significativamente del promedio. Para mejorar el código y hacerlo más eficiente, especialmente cuando se supervise un gran número de cuentas, propongo las siguientes mejoras:

Optimización para múltiples usuarios: En lugar de analizar los inicios de sesión para un solo usuario, se podría adaptar el código para procesar múltiples usuarios a la vez. Esto haría que el sistema sea escalable y capaz de manejar grandes volúmenes de datos.

Uso de bases de datos: Para almacenar y consultar los datos de inicio de sesión de manera eficiente, recomendaría almacenar los registros en una base de datos (por ejemplo, SQL o NoSQL). Esto optimiza la búsqueda de patrones y la gestión de grandes cantidades de datos de múltiples usuarios.

Límites dinámicos: En lugar de usar un umbral fijo de 3 para la relación de inicios de sesión, se podría implementar un umbral dinámico basado en el comportamiento histórico del usuario, lo que permitiría ajustar el sistema según las fluctuaciones en el comportamiento del usuario a lo largo del tiempo.

Seguridad: Para garantizar que el código esté alineado con las mejores prácticas de seguridad, se recomienda realizar un análisis de seguridad en el código. Referencias como las del OWASP Top Ten y NIST SP 800-53 pueden guiar sobre cómo proteger la aplicación frente a posibles vulnerabilidades, como ataques de inyección de código o acceso no autorizado.

Manejo de excepciones y validación de entrada: Asegúrese de manejar excepciones adecuadas, como cuando no haya datos de inicio de sesión o cuando los datos proporcionados sean incorrectos. Esto evitará caídas del sistema y proporcionará información útil en los registros.

Contexto adicional: Este código se ejecutará en un entorno de alta disponibilidad, donde la eficiencia y la escalabilidad son esenciales. Además, las alertas generadas deben ser precisas para evitar falsas alarmas y para permitir una respuesta rápida por parte del equipo de seguridad.

Referencias:
OWASP Top Ten: Para proteger contra vulnerabilidades comunes.
NIST SP 800-53: Proporciona pautas de seguridad recomendadas para sistemas de información.

3. 3. ¿Cómo afectaron la evaluación y la iteración al resultado final? *Escribe 1-2 frases.* **1 / 1 punto**

La evaluación y la iteración permitieron identificar áreas clave para mejorar el código, como la escalabilidad, la seguridad y el rendimiento. La evaluación constante y la retroalimentación ayudarán a refinar el enfoque, haciendo que el resultado final sea más robusto y alineado con las mejores prácticas de la industria.