Desafío - Técnicas de redacción concisas

En este desafío validaremos nuestros conocimientos en las técnicas de redacción clara y concisa en la documentación de hallazgos de seguridad, utilizando herramientas que permita apoyar la redacción respectiva. Para lograrlo, necesitarás aplicar los requerimientos solicitados.

Lee todo el documento antes de comenzar el desarrollo **individual** para asegurarte de tener el máximo de puntaje y enfocar bien los esfuerzos.

// Tiempo asociado: 1 hora cronológica

Descripción

La empresa **TechSecure** ha detectado actividad inusual en su red. Un usuario reportó que su cuenta fue utilizada para acceder a datos confidenciales sin su autorización. El equipo de seguridad realizó un análisis inicial y encontró los siguientes hallazgos:

- **Credenciales filtradas**: Se detectaron intentos de acceso desde una ubicación sospechosa
- **Falta de autenticación multifactor (MFA)**: Las cuentas comprometidas no tenían un segundo factor de autenticación.
- **Exfiltración de datos**: Se identificó tráfico inusual hacia una IP externa desconocida**.**
- **Uso de un malware tipo keylogger**: Se sospecha que un empleado fue víctima de phishing y ejecutó un archivo malicioso.

Requerimientos

1. Redactar un informe, evitando términos complejos e innecesarios. El informe debe tener las secciones de resumen del incidente, análisis de la situación, hallazgos claves y medidas correctivas propuestas.
   (**2 Puntos**)

2. En el informe crear al menos una tabla para resumir los hallazgos o las recomendaciones. Usar un diagrama de flujo para representar como ocurrió el ataque, además de apoyar con un gráfico para visualizar el impacto del incidente.
   (**2 Puntos**)

3. Utilizar herramientas como Gammarly, Hemigway o IA para revisar la claridad y la gramática del informe. Evidencias las mejoras. (**3 Puntos**)

4. En el informe incluir una conclusión de lo realizado en el caso planteado. (**3 Puntos**)

 ¡Mucho éxito!

Consideraciones y recomendaciones