Desafío - Riesgos de seguridad en entornos corporativos

En este desafío validaremos nuestros conocimientos en analizar los elementos fundamentales de la seguridad en redes para identificar y evaluar los riesgos asociados en un entorno corporativo. 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 (Si el desafío se desarrolla por los estudiantes en menos tiempo del indicado, se debe realizar la creación de uno adicional para completar el tiempo indicado de la sesión).

Descripción

Leer el siguiente caso y responder las preguntas propuestas en un documento Word.

Eres un especialista en ciberseguridad de una empresa de comercio electrónico llamada "**FastBuy**", que maneja miles de transacciones diarias y almacena información sensible de clientes, como datos personales y bancarios.

En la última semana, el equipo de TI ha detectado varias anomalías en la red, lo que ha generado preocupación sobre un posible ataque en curso. Se han reportado los siguientes incidentes:

- **Incremento inusual en el tráfico del servidor web**, provocando lentitud y caídas intermitentes del servicio.
- **Correos electrónicos sospechosos** enviados a empleados con enlaces fraudulentos solicitando credenciales.
- **Registros en el firewall que muestran intentos repetidos de acceso no autorizado** a la base de datos.
- **Inyecciones de código** detectadas en los formularios de inicio de sesión de la plataforma.

Requerimientos

1. Explicar la importancia de la seguridad de la red en la empresa de comercio electrónico FastBuy. Además de describir como la confidencialidad, integridad y disponibilidad se ven afectados
(**2 Puntos**)

2. Identificar y describir los activos más críticos para la empresa FastBuy (servidores, bases de datos, dispositivos de red). Clasificar los activos en función de su criticidad y justificar la clasificación realizada. (**2 Puntos**)

3. Analizar los tipis de ataques que se están produciendo en Fastbuy y clasificarlos. También explicar el método que podrían haber utilizado los atacantes para llevar a cabo los ataques. (**2 Puntos**)

4. Identificar los riesgos específicos que estos ataques representan para Fastbuy. Además de evaluar el impacto potencia y la probabilidad de cada amenaza, asignándole una clasificación de bajo, medio o alto según es necesario. (**2 Puntos**)

5. Proponer 2 estrategias para mejorar la resiliencia y disponibilidad en la red Fastbuy ante futuros ataques. (**2 Puntos**)

 ¡Mucho éxito!

Consideraciones y recomendaciones