Prueba de conocimientos

5 minutos

Elija la respuesta más adecuada para cada una de las preguntas siguientes. Después, seleccione **Comprobar las respuestas**.

Comprobación de conocimientos

1. ¿Dónde se pueden crear y administrar alertas de seguridad personalizadas?

- ○ Azure Security Center
- ◉ Azure Sentinel

  ✔ **Azure Sentinel. Las reglas de alerta personalizadas se retiraron de Azure Security Center el 30 de junio de 2019 porque se retiró su infraestructura subyacente. Se recomienda habilitar Azure Sentinel y volver a crear allí las alertas personalizadas. Como alternativa, las alertas se pueden crear con alertas de registro de Azure Monitor.**

- ○ Almacenamiento de Azure

2. ¿Cuál de los siguientes elementos superaría las funcionalidades de un cuaderno de estrategias de Azure Sentinel?

- ○ Un cuaderno de estrategias de Sentinel puede ayudar a automatizar y organizar una respuesta a incidentes.
- ○ Un cuaderno de estrategias de Sentinel se puede ejecutar manualmente o establecer para ejecutarse automáticamente cuando se desencadenan alertas específicas.
- ◉ Se creará un cuaderno de estrategias de Sentinel para controlar varias suscripciones a la vez.

  ✔ **Un cuaderno de estrategias de seguridad es una colección de procedimientos que se pueden ejecutar desde Azure Sentinel en**

respuesta a una alerta. Un cuaderno de estrategias de seguridad puede ayudar a automatizar y orquestar la respuesta y se puede ejecutar manualmente o establecer para ejecutarse automáticamente cuando se desencadenan alertas específicas. Cada cuaderno de estrategias se crea para una suscripción específica.

3. Sentinel se usa para investigar un incidente. Al ver la información detallada del incidente, ¿qué valor se debe asignar, en lugar de incluirse en los datos?

- ○ Identificador de incidente
- ◉ Propietario de un incidente

  ✔ **Propietario de un incidente. La información detallada del incidente incluye su gravedad, el resumen del número de entidades implicadas, los eventos sin procesar que desencadenaron este incidente y el identificador único del incidente. Todos los incidentes se inician sin tener un propietario asignado. Cada incidente se puede asignar a un propietario estableciendo el campo Propietario del incidente. También se pueden agregar comentarios para que otros analistas puedan comprender lo que se investigó y cuáles son sus preocupaciones en torno al incidente.**
- ○ Número de entidades implicadas

4. Al crear roles dentro de un equipo de operaciones de seguridad para conceder el acceso adecuado a Azure Sentinel. ¿Cuál de los roles siguientes tendría que crearse en lugar de integrarse?

- ○ Lector de Azure Sentinel
- ○ Respondedor de Azure Sentinel
- ◉ Propietario de Azure Sentinel

  ✔ **Los roles integrados de Sentinel son lector, respondedor y colaborador.**

5. Un investigador quiere ser proactivo a la hora de buscar amenazas de seguridad. El responsable de seguridad ha leído sobre las funcionalidades de búsqueda y los cuadernos de Sentinel. ¿Qué es un cuaderno de Azure Sentinel?

- ◉ Un cuaderno de estrategias paso a paso que proporciona la capacidad de seguir los pasos de una investigación y búsqueda.

✔ **Un cuaderno de estrategias paso a paso. Un cuaderno es un cuaderno de estrategias paso a paso que permite seguir los pasos de una investigación y búsqueda. Otras técnicas de búsqueda se describen en las otras opciones: consulta integrada, marcadores y tablas de eventos.**

○ Una tabla para consultar y localizar acciones como eventos DNS.

○ Un elemento guardado para la creación de un incidente para su investigación.

Siguiente unidad: Resumen

Continuar >

¿Cómo lo estamos haciendo? ☆ ☆ ☆ ☆ ☆