

## ✓ ¡Felicitaciones! ¡Aprobaste!

Calificación recibida 100 % Para Aprobar 75 % o más

Ir al siguiente elemento

Para aprobar esta práctica, debes obtener un puntaje de al menos el 75%, o 3 de 4 puntos, completando la actividad y respondiendo a las preguntas del cuestionario. Una vez que completes el cuestionario, revisa los comentarios. Puedes conocer más sobre las prácticas y ejercicios con calificación en la [descripción general del curso](#) [↗](#).



### Resumen de la actividad

En esta actividad, te presentaremos la plataforma Splunk. A continuación, usarás Splunk Cloud para subir datos, realizar búsquedas básicas en ellos y responder a una serie de preguntas. Antes de comenzar a usar Splunk, tendrás que hacer lo siguiente:

- Crear una cuenta de Splunk.
- Activar una prueba gratuita de Splunk Cloud.
- Cargar datos en Splunk Cloud.

**Ten en cuenta que esta actividad es opcional y no influirá en la finalización del curso.**

Hasta ahora, aprendiste que las herramientas SIEM, como Splunk, son una parte importante de la caja de herramientas de un analista de seguridad, ya que proporcionan una plataforma para almacenar, analizar y generar informes sobre datos de diferentes fuentes. También, exploraste algunas búsquedas básicas utilizando el lenguaje de consulta de Splunk, llamado Search Processing Language (SPL), que incluye el uso de tuberías y comodines.

La creación de búsquedas efectivas es una habilidad importante porque te permite encontrar con rapidez y precisión la información que estás buscando dentro de una gran cantidad de datos. Las búsquedas rápidas y precisas son útiles durante la respuesta a incidentes, ya que puede ser necesario identificar y abordar rápidamente un incidente de seguridad. Las técnicas de búsqueda eficaces también ayudan a identificar patrones, tendencias y anomalías en los datos.

### Escenario

Revisa el siguiente escenario. Luego, completa las instrucciones paso a paso.

Eres analista de seguridad y trabajas en la tienda de comercio electrónico Buttercup Games. Te han encargado identificar si existen posibles problemas de seguridad en el servidor de correo. Para ello, debes explorar cualquier inicio de sesión SSH fallido para la cuenta root.

**Nota:** Utiliza el diario de gestión de incidentes que iniciaste en [una actividad anterior](#) [↗](#) para tomar notas durante la actividad y hacer un seguimiento de tus hallazgos.

### Instrucciones paso a paso

Sigue las instrucciones y responde a las siguientes preguntas para completar la actividad.

- > Paso 1: Accede a los materiales de apoyo
- > Paso 2: Crea una cuenta de Splunk
- > Paso 3: Regístrate para obtener una prueba gratuita de Splunk Cloud
- > Paso 4: Sube los datos en Splunk

> Paso 5: Realiza una búsqueda básica

> Paso 6: Evalúa los campos

> Paso 7: Limita tu búsqueda

> Paso 8: Busca un inicio de sesión fallido para root

> Paso 9: Evalúa los resultados de búsqueda

#### Paso 10: Responde a las preguntas sobre los resultados de búsqueda

1. ¿Cuántos eventos se albergan en el índice principal en todo momento?

1 / 1 punto

- ☐ 10,000
- ☐ 100-1000
- ☐ 10-99
- ☒ Más de 100,000

✓ Correcto

Si ingresas una búsqueda de todos los eventos en el índice principal, recuperarás 109,864 eventos.

2. ¿Qué campo identifica el nombre de un dispositivo de red o sistema desde el que se origina un evento?

1 / 1 punto

- ☐ sourcetype
- ☐ source
- ☐ index
- ☒ host

✓ Correcto

El campo `host` especifica el nombre de un host, como un dispositivo de red u otro sistema, desde donde se origina un evento.

3. ¿Cuál de los siguientes hosts utilizados por Buttercup Games contiene información de registro relevante para transacciones financieras?

1 / 1 punto

- ☐ `www2`
- ☐ `www1`
- ☒ `vendor_sales`
- ☐ `www3`

✓ Correcto

El host `vendor_sales` ofrece información sobre las ventas minoristas de Buttercup Games, como la cantidad de productos vendidos.

4. ¿Cuántos inicios de sesión SSH fallidos hay para la cuenta root (cuenta raíz) en el servidor de correo?

1 / 1 punto

- ☐ Ninguno
- ☐ Uno
- ☐ 100




**Correcto**

Hay más de 100 inicios de sesión SSH fallidos para la cuenta root en el servidor de correo.

## Conclusiones clave

En esta actividad, utilizaste Splunk Cloud para realizar una búsqueda e investigación. Usando Splunk Cloud, pudiste:

- Cargar datos de registro de muestra.
- Buscar en los datos indexados.
- Evaluar los resultados de búsqueda.
- Identificar las diferentes fuentes de datos.
- Localizar los inicios de sesión SSH fallidos para la cuenta root.

Si deseas plantearte desafíos y explorar más investigaciones de incidentes simulados usando Splunk, inicia sesión en Splunk y visita [Splunk Boss del SOC](#) .