¡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 4,6 de 6 puntos, completando la actividad y respondiendo a las preguntas correspondientes. 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, utilizarás Chronicle, una herramienta nativa de la nube, para investigar un incidente de seguridad relacionado con la suplantación de identidad y responder a una serie de preguntas.

Anteriormente, aprendiste cómo las herramientas SIEM, como Chronicle, proporcionan una plataforma para recopilar, analizar y generar informes sobre datos de diferentes fuentes. Como analista de seguridad, usarás herramientas SIEM para identificar y responder a incidentes de seguridad.

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

Escenario

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

Eres analista de seguridad en una empresa de servicios financieros. Te llega una alerta de que un empleado recibió un correo electrónico de phishing en su bandeja de entrada. La revisas e identificas un nombre de dominio sospechoso en el cuerpo del correo electrónico: signin.office365x24.com. Debes determinar si otros empleados han recibido correos electrónicos de phishing que contengan este dominio y si lo han visitado. Utilizarás Chronicle para investigar este dominio.

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 preguntas para completar la actividad.

Paso 1: Inicia Chronicle

Paso 2: Realiza una búsqueda de dominio

Paso 3: Evalúa los resultados de búsqueda

Paso 4: Investiga los datos de inteligencia de amenazas

Paso 5: Investiga los activos y eventos afectados

Paso 6: Investiga la dirección IP resuelta

Paso 7: Responde a las preguntas sobre la investigación del dominio

Conclusiones clave

En esta actividad, utilizaste Chronicle para investigar un dominio sospechoso utilizado en un correo electrónico de phishing. Mediante la búsqueda de dominio de Chronicle, pudiste:

- Acceder a informes de inteligencia de amenazas sobre el dominio.
- Identificar los activos que accedieron al dominio.
- Evaluar los eventos HTTP asociados al dominio.
- Identificar qué activos enviaron información de inicio de sesión al dominio.
- Identificar dominios adicionales.

Tras la investigación, determinaste que el dominio sospechoso ha estado involucrado en campañas de phishing. También, que varios activos podrían haberse visto afectados por la campaña de phishing, ya que los registros mostraban que se había enviado información de inicio de sesión al dominio sospechoso a través de solicitudes `POST`. Finalmente, identificaste dos dominios adicionales relacionados con el dominio sospechoso al examinar la dirección IP resuelta.

Si deseas seguir investigando, consulta la función de chatbot en la página de inicio de Chronicle.

1. Según la lista de representantes de inteligencia sobre amenazas emergentes (ET) disponible, ¿cómo se categoriza `signin.office365x24.com`? **1 / 1 punto**

- ○ Sitio de spam
- ○ Sitio de phishing
- ○ Servidor de comandos y control
- ◉ Sitio de entrega para registros o credenciales robadas

Correcto
La tarjeta de información categoriza el comportamiento de `signin.office365x24.com` como un sitio de entrega para registros o credenciales robadas. Esto significa que se ha informado de que este dominio envía y recibe credenciales robadas u otros datos.

2. ¿Qué activos accedieron al dominio `signin.office365x24.com`? Selecciona tres respuestas. **1 / 1 punto**

- ☑ `roger-spence-pc`

Correcto
`roger-spence-pc`, `emil-palmer-pc` y `coral-alvarez-pc` son tres de los seis activos que accedieron a este dominio.

- ☐ `thomas-garcia-pc`
- ☑ `coral-alvarez-pc`

Correcto
`roger-spence-pc`, `emil-palmer-pc` y `coral-alvarez-pc` son tres de los seis activos que accedieron a este dominio.

- ☑ `emil-palmer-pc`

Correcto
`roger-spence-pc`, `emil-palmer-pc` y `coral-alvarez-pc` son tres de los seis activos que accedieron a este dominio.

3. ¿A qué dirección IP lleva el dominio `signin.office365x24.com`? **1 / 1 punto**

- ○ `45.32.8.8`
- ◉ `40.100.174.34`
- ○ `10.0.0.222`
- ○ `10.0.29.22`

Correcto
`signin.office365x24.com` lleva a la dirección IP `40.100.174.34`.

4. ¿Cuántas solicitudes `POST` se realizaron al dominio `signin.office365x24.com`? **1 / 1 punto**

- ○ 8
- ○ 6
- ◉ 2
- ○ 1

Correcto
Se realizaron dos solicitudes `POST` al dominio `signin.office365x24.com`. Esto indica que se envió información sensible, como credenciales de inicio de sesión, a la página de inicio de sesión.

5. Se realizaron algunas solicitudes `POST` a `signin.office365x24.com`. ¿Cuál es la URL de destino de la página web a la que se realizaron las solicitudes `POST`? **1 / 1 punto**

- ○ `http://accounts-gooqle.com/login.php`
- ○ `http://office365x24.com/login.exe`
- ◉ `http://signin.office365x24.com/login.php`
- ○ `http://accounts-gooqle.com/login.txt`

Correcto
Las solicitudes `POST` se enviaron a `http://signin.office365x24.com/login.php`.

6. ¿A qué dominios lleva la dirección IP `40.100.174.34`? Selecciona dos respuestas. **1 / 1 punto**

- ☐ `cloud2.xdnscloud.com`
- ☐ `euw.adserver.snapads.com`
- ☑ `signin.office365x24.com`

Correcto
`40.100.174.34` lleva a `signin.accounts-gooqle.com` y `signin.office365x24.com`.

- ☑ `signin.accounts-gooqle.com`

Correcto
`40.100.174.34` lleva a `signin.accounts-gooqle.com` y `signin.office365x24.com`.