Introducción a la seguridad de endpoints

En esta sala, presentaremos los fundamentos de la monitorización de la seguridad de endpoints, las herramientas esenciales y la metodología general. Ofreceremos una visión general de cómo identificar una actividad maliciosa desde un endpoint y mapear sus eventos relacionados.
Para comenzar, abordaremos los siguientes temas para sentar las bases sobre cómo abordar la supervisión de seguridad de endpoints.

- Fundamentos de seguridad de endpoints
- Registro y monitoreo de puntos finales
- Análisis de registros de puntos finales

Al final de esta sala, realizaremos una simulación de amenazas en la que deberá investigar y remediar las máquinas infectadas. Para completar esta actividad, es posible que primero deba comprender los fundamentos de la monitorización de la seguridad de endpoints.
¡Ahora, profundicemos en los conceptos básicos de seguridad de endpoints!

Tarea 1: Introducción a la sala
P: He leído la tarea de introducción.
R: No se necesita respuesta

Tarea 2: Fundamentos de seguridad de endpoints
P1: ¿Cuál es el proceso padre normal de services.exe?
R1: wininit.exe

P2: ¿Cuál es el nombre de la herramienta de utilidad de red presentada en esta tarea?
R2: TCPView

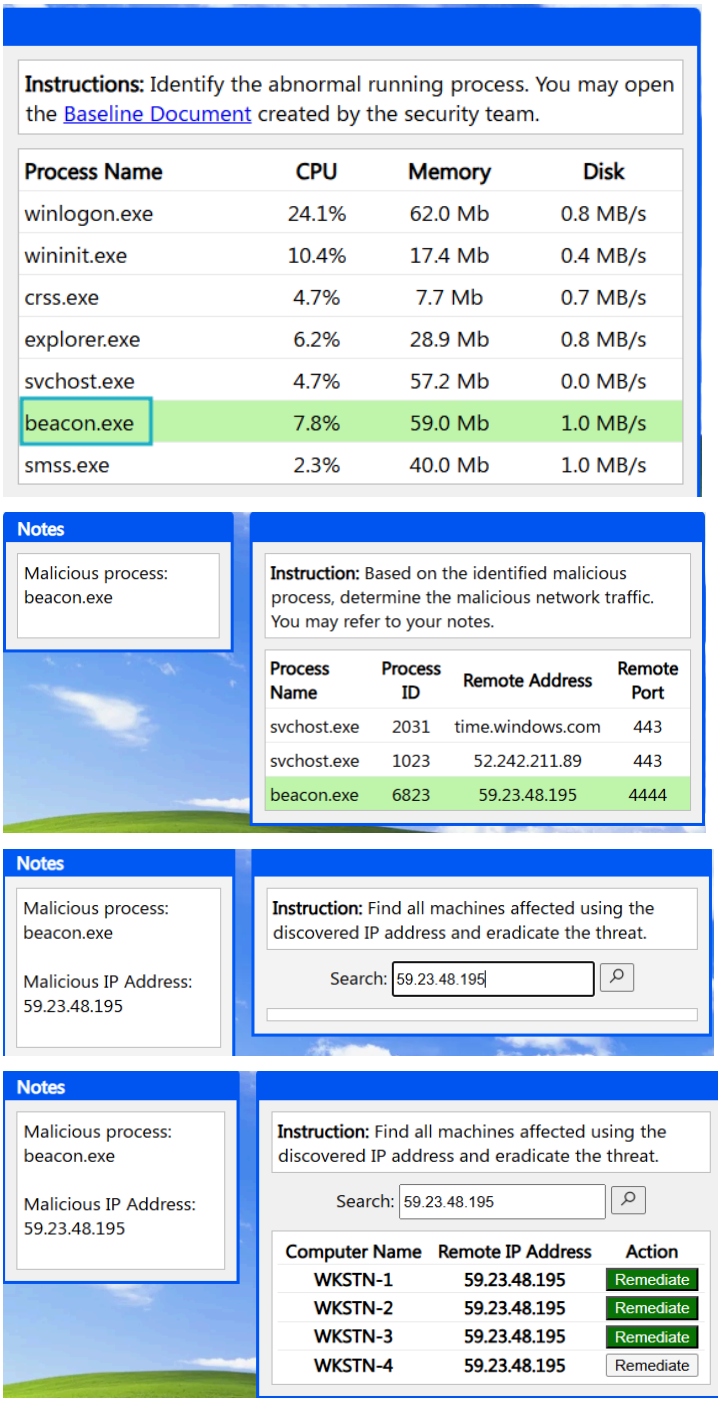
Tarea 3: Registro y monitoreo de puntos finales
P1: ¿Dónde residen normalmente los registros de eventos de Windows (archivos .evtx)?
R1: C:\Windows\System32\winevt\Logs

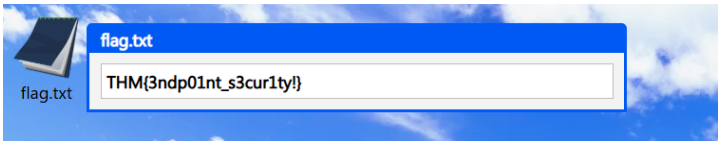
P2: Proporcione el comando utilizado para ingresar a OSQuery CLI.
R2: osqueryi

P3: ¿Qué significa EDR? Responde con minúsculas.
R3: endpoint detection and response / detección y respuesta de puntos finales

Tarea 4: Análisis de registros de puntos finales
P1: Haga clic en el botón verde Ver sitio en esta tarea para abrir el Laboratorio del sitio estático y comenzar a investigar la amenaza siguiendo las instrucciones proporcionadas.
R1: No se necesita respuesta

P2: Proporcionar la bandera para la actividad de investigación simulada.





R2: THM{3ndp01nt_s3cur1ty!}

Tarea 5: Conclusión

¡Felicitaciones! Has completado la tarea de investigación.

En la actividad de investigación de amenazas simuladas, hemos aprendido lo siguiente:

- Tener un documento de referencia le ayudará a diferenciar los eventos maliciosos de los benignos.
- La correlación de eventos proporciona una comprensión más profunda de los eventos simultáneos desencadenados por la actividad maliciosa.
- Tomar nota de cada artefacto significativo es crucial en la investigación.
- Se deben inspeccionar y remediar otros activos potencialmente afectados utilizando los artefactos maliciosos recopilados.

En conclusión, cubrimos los conceptos básicos de Monitoreo de Seguridad de Endpoints:

- **Los fundamentos de seguridad de endpoints** abordaron los procesos centrales de Windows y Sysinternals.
- **Endpoint Logging and Monitoring** introdujo funcionalidades de registro como Windows Event Logging y Sysmon y herramientas de monitoreo/investigación como OSQuery y Wazuh .
- **El análisis del registro de puntos finales** destacó la importancia de tener una metodología como la base de referencia y la correlación de eventos.

Ya está listo para profundizar en el módulo de monitorización de seguridad de endpoints. Para continuar, puede consultar la lista de salas mencionada en las tareas anteriores:

- Procesos centrales de Windows
- Sysinternals
- Registros de eventos de Windows
- Sysmon
- Consulta OS
- Wazuh

P: He completado la sala de Introducción a la Monitorización de Seguridad de Endpoints.
R: No se necesita respuesta

💼**LinkedIn:**https://www.linkedin.com/in/mateo-rodr%C3%ADguez-suar-202695249/
💻 **GitHub:** https://github.com/MaateoSuar