Lab - Recomendar medidas de seguridad de

NOTA: RESPONDER CADA PREGUNTA CON CAPTURAS DE PANTALLA COMPLETAS DONDE SE VEAN LAS SIGLAS DE SU NOMBRE AL LADO DEL RELOJ. EN LUGAR DE COLOCAR UN TEXTO DEBE DE SELECCIONAR EL TEXTO INVESTIGADO EN UNA PÁGINA WEB Y HACERLE CAPTURA DE PANTALLA COMPLETA, PARA LUEGO COLOCARLA AQUÍ. SI SON VARIAS PREGUNTAS, DEBE COLOCAR VARIAS CAPTURAS DE PANTALLAS COMPLETAS. NO COLOCAR INFORMACIÓN ENCONTRADA EN NETACAD, COLOCAR INFORMACIÓN INVESTIGADA EN OTRAS PÁGINAS WEB O LO REALIZADO POR USTED.

Objetivos

Parte 1: Recomendar procedimientos de mitigación para abordar las vulnerabilidades

Parte 2: recomendar un producto de protección de terminales para una nueva red

Aspectos básicos/Situación

Para proporcionar seguridad, los profesionales generalmente implementan una serie de medidas de seguridad de la red que funcionan en conjunto en un enfoque de seguridad por capas. Los firewalls y otros dispositivos protegen el perímetro de la red contra ataques; sin embargo, siempre es posible que las amenazas puedan eludir estas defensas. Por lo tanto, no solo es necesario proteger el perímetro de la red, sino también tomar medidas para proteger los hosts de red individuales contra riesgos. En esta práctica de laboratorio, leerá dos casos de estudio y recomendará mitigaciones de amenazas de terminales que sean adecuadas para abordar los ataques.

Recursos necesarios

- Acceso a Internet

Instrucciones

Parte 1: Recomendar procedimientos de mitigación para abordar las vulnerabilidades

Usted trabaja en un equipo de seguridad para una empresa de fabricación. Un cliente nuevo requiere que, antes de que la empresa pueda recibir el contrato, cumpla con estándares más estrictos. Se completó una evaluación de vulnerabilidades de la red y se encontraron varias vulnerabilidades, incluidos los siguientes problemas de seguridad de terminales:

- La empresa utiliza sistemas de control de supervisión y adquisición de datos (SCADA) para supervisar y controlar sus procesos de fabricación. El software SCADA se ejecuta en el sistema operativo Windows XP.
- Los sistemas críticos permiten el uso de medios USB desconocidos.
- Los usuarios pueden acceder a la red con dispositivos de computación personal, como smartphones, tablets y computadoras portátiles.
- Los usuarios pueden navegar libremente por la WWW, incluidos los sitios de malware conocidos.
- El software antivirus inconsistente instalado en los hosts incluía versiones antiguas con un estado de actualización de firma desconocido.

Con el material cubierto en este curso y la información adicional que encuentra en Internet, complete la tabla a continuación.

Asunto	Recomendación
Versiones obsoletas del sistema operativo	Es importante reemplazar los sistemas que todavía usan Windows XP, ya que este sistema ya no recibe actualizaciones de seguridad. Se recomienda migrar a versiones más recientes, como Windows 10 IoT o incluso Linux en los entornos SCADA. Mientras tanto, estos equipos deben mantenerse en una red aislada y con acceso limitado para reducir el riesgo de ataques.
Los sistemas críticos permiten el uso de medios USB	Para evitar la propagación de malware, se debe bloquear el uso de memorias USB no autorizadas mediante políticas de grupo o configuraciones de BIOS. En los casos donde sea necesario usarlas, se debe implementar un control de dispositivos que permita solo los USB aprobados y que analice automáticamente los archivos antes de abrirlos.
Uso de dispositivos de computación personal en la red	Los empleados que necesiten conectar sus dispositivos personales (como celulares o laptops) deben hacerlo en una red separada de la red principal de la empresa. Además, se recomienda aplicar políticas BYOD (Bring Your Own Device) y usar herramientas de administración de dispositivos móviles (MDM) para asegurar que los equipos cumplan con las normas de seguridad.
Los usuarios pueden navegar libremente por la WWW	Se deben aplicar restricciones de navegación mediante un filtro de contenido o proxy web, para evitar el acceso a sitios maliciosos o no relacionados con el trabajo. También es recomendable usar un sistema de DNS seguro (como Cisco Umbrella o Cloudflare) que bloquee automáticamente dominios sospechosos.
Problemas de antivirus	Todos los equipos deben contar con una misma solución de antivirus actualizada y configurada para realizar análisis automáticos. Lo ideal sería usar una solución más avanzada, como un sistema EDR (Endpoint Detection and Response), que pueda detectar comportamientos sospechosos y responder de forma rápida ante posibles amenazas.

Parte 2: Recomendar un producto de protección de terminales para una nueva red

Un amigo ha recibido recientemente fondos de capital de riesgo para un nuevo producto prometedor. Se prevé un rápido crecimiento. Está abriendo una ubicación para su inicio y le ha pedido que lo ayude con recomendaciones sobre medidas de seguridad de terminales para implementar en la nueva red.

Utilice su aprendizaje en el curso e investigue en Internet para recomendar un producto de seguridad integral para terminales. Tenga en cuenta que la empresa actualmente es pequeña, pero crecerá rápidamente. Proporcione los motivos de su decisión según las características del producto.

Registre su producto elegido:

Característica	Valor
Tipo de protección	Ofrece protección completa contra virus, ransomware, phishing, ataques de red y comportamientos sospechosos. Incluye antivirus, firewall, control de aplicaciones y Sistema EDR.
Facilidad de gestión	Permite administrar todos los equipos desde una sola consola en la nube, donde se pueden revisar alertas, aplicar políticas y responder a incidentes en tiempo real.
Escalabilidad	Es ideal para empresas pequeñas que planean crecer rápidamente, ya que se adapta fácilmente a nuevos dispositivos y usuarios sin necesidad de infraestructura adicional.
Compatibilidad	Funciona en Windows, macOS, Android y Linux, y se integra fácilmente con Microsoft 365 y Azure, lo que facilita la administración centralizada.
Prevención avanzada	Utiliza inteligencia artificial y análisis de comportamiento para detectar amenazas incluso antes de que causen daño. También puede aislar equipos comprometidos para evitar que el ataque se propague.
Costo y beneficio	Tiene un costo razonable y ofrece una protección sólida con características empresariales, sin necesidad de grandes inversiones iniciales.
Conclusion	Se recomienda Microsoft Defender for Endpoint por su facilidad de uso, alta efectividad y capacidad para crecer junto con la empresa, garantizando una protección moderna y confiable para los equipos.