Domain 7 - Security Operations

Test ID: 178688630

Pregunta #1 de 163

Id. de pregunta: 1192971

Su organización está considerando la posibilidad de alquilar un centro de datos externo para proporcionar recuperación de instalaciones si se produce un desastre. La administración desea arrendar un sitio frío. ¿Cuáles son algunas desventajas de este tipo de sitio?

a. gastos

b. tiempo de recuperación

c. tiempo de administración

d. Disponibilidad de las pruebas

- ✗ **A)** opción A
- ✗ **B)** opción b
- ✗ **C)** Opción d
- ✗ **D)** opción c
- ✓ **E)** Opciones B y D
- ✗ **F)** Opciones A y C

Explicación

Los sitios fríos tardan mucho tiempo en ponerse en línea. Tampoco están tan disponibles para las pruebas como otras alternativas. Por lo tanto, el tiempo de recuperación y la disponibilidad de pruebas son dos desventajas en el uso de un sitio frío.

Los sitios fríos son baratos y no requieren tiempo de administración diario. Por lo tanto, el gasto y el tiempo de administración son dos ventajas en el uso de un sitio frío.

Los sitios calientes son caros. Requieren mucho tiempo de administración para garantizar que el sitio esté listo dentro del tiempo de inactividad máximo tolerable (MTD). Por lo tanto, el gasto y el tiempo de administración son dos desventajas en el uso de un sitio caliente. Además, otra desventaja de un sitio caliente es que necesitaría amplios controles de seguridad.

Los sitios calientes están disponibles dentro del MTD y están disponibles para la prueba. Por lo tanto, el tiempo de recuperación y la disponibilidad de pruebas son dos ventajas en el uso de un sitio caliente.

Los sitios cálidos son menos costosos que los sitios calientes, pero más caros que los sitios fríos. El tiempo de recuperación de un sitio cálido es más de lo que se necesita para un sitio caliente, pero menor que el necesario para

un sitio frío. Los sitios calientes requieren generalmente menos tiempo de administración porque solamente se mantiene el equipo de las telecomunicaciones, no el equipo informático. Los sitios cálidos son más fáciles de probar que los sitios fríos, pero más difíciles de probar que los sitios calientes.

Los sitios redundantes son caros y requieren mucho tiempo de administración. Sin embargo, requieren un pequeño tiempo de recuperación y son más fáciles de probar que las instalaciones propiedad de otras empresas.

Objetivo:
Operaciones de seguridad

Subobsecución:
Probar planes de recuperación ante desastres (DRP)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, recuperación y estrategias de múltiples sitios

---

Pregunta #2 de 163

Id. de pregunta: 1111779

Se le ha pedido que reduzca el área expuesta de un equipo con Windows Server 2012 que actúa como servidor web. ¿Qué paso NO se incluye en la reducción de los ataques de área expuesta?

- ✗ **A)** Deshabilite los servicios innecesarios.
- ✗ **B)** Utilice privilegios mínimos.
- ✗ **C)** Deshabilite los protocolos innecesarios.
- ✓ **D)** Deshabilite la auditoría.

Explicación

No debe deshabilitar la auditoría. La auditoría debe implementarse para registrar eventos que podrían poner en peligro la seguridad. Sin auditoría, no tiene forma de realizar un seguimiento de los eventos que se producen.

La reducción de los ataques de área expuesta incluye los siguientes pasos:

- Deshabilite los servicios innecesarios.
- Deshabilite los protocolos innecesarios.
- Utilice privilegios mínimos.
- Aplicar la defensa en profundidad.
- No confíe en los datos proporcionados por el usuario.
- Falla de forma segura.
- Asegure el eslabón más débil.

- Crear valores predeterminados seguros.

Los servicios y protocolos innecesarios pueden permitir fácilmente que los piratas informáticos accedan a sus servidores. Un analizador de puertos puede identificar qué servicios y protocolos se están ejecutando para que pueda deshabilitar los servicios y protocolos innecesarios.

Objetivo:
Operaciones de seguridad

Subobsecución:
aprovisionamiento seguro de recursos

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 7: Operaciones de seguridad, endurecimiento del sistema

Fundamentos de seguridad de aplicaciones web, http://msdn.microsoft.com/en-us/library/aa302417.aspx

---

Pregunta #3 de 163

Id. de pregunta: 1105417

Se le ha pedido que proporcione una copia de un acuerdo contractual entre su organización y un tercero. ¿Qué tipo de evidencia representa este documento?

✗ **A)** mejor evidencia
✓ **B)** evidencia secundaria
✗ **C)** pruebas de oídas
✗ **D)** pruebas concluyentes

Explicación

Las copias de los acuerdos contractuales se denominan pruebas secundarias y no mejores pruebas.

Una copia original del acuerdo contractual se denomina la mejor evidencia. La mejor evidencia o la evidencia real es la pieza de evidencia que tiene el mayor grado de confiabilidad.

Por otro lado, la evidencia secundaria no se considera igualmente confiable y fuerte porque la evidencia puede ser manipulada. La evidencia oral generalmente cae en esta categoría.

La evidencia concluyente se refiere a una pieza de evidencia que no requiere ninguna corroboración y es completa en sí misma. Este tipo de pruebas no pueden ser impugnadas.

La evidencia de oídas se refiere a la evidencia que no tiene prueba de exactitud o confiabilidad. Por ejemplo, un testigo que proporciona testimonio oral basado en lo que esa persona ha escuchado de otra persona se considera

evidencia de oídas.

Objetivo:

Operaciones de seguridad

Subobsecución:

Comprender los requisitos para los tipos de investigación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, evidencia secundaria

---

Pregunta #4 de 163

Id. de pregunta: 1111793

¿Qué principio estipula que no se deben realizar múltiples cambios en un sistema informático al mismo tiempo?

- ✗ **A)** atención debida
- ✗ **B)** Debida diligencia
- ✗ **C)** uso aceptable
- ✓ **D)** gestión de cambios

Explicación

La administración de cambios estipula que no se deben realizar múltiples cambios en un sistema informático al mismo tiempo. Esto hace que el seguimiento de cualquier problema que pueda ocurrir sea mucho más sencillo. La administración de cambios incluye las siguientes reglas:

- Distinga entre los tipos de sistema.
- Documente el proceso de cambio.
- Desarrolle los cambios en función de la configuración actual.
- Pruebe siempre los cambios.
- NO realice más de un cambio a la vez.
- Documente su plan de reserva.
- Asigne a una persona responsable de la gestión de cambios.
- Informar regularmente sobre el estado de la gestión del cambio.

Objetivo:

Operaciones de seguridad

Subobsecución:
Comprender y participar en los procesos de gestión del cambio

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 7: Operaciones de seguridad, procesos de gestión de cambios

---

Pregunta #5 de 163

Id. de pregunta: 1114772

Como parte de la directiva de seguridad de su organización, debe supervisar las infracciones de control de acceso. ¿Qué método(s) debe(n) utilizar?

a. ACL

b. IDSs

c. Copias de seguridad

d. Registros de auditoría

- ✗ **A)** Opción d
- ✗ **B)** opción c
- ✗ **C)** opción A
- ✗ **D)** opción b
- ✗ **E)** todas las opciones
- ✓ **F)** Opciones B y D Sólo
- ✗ **G)** opciones b, c y d solamente

Explicación

Los sistemas de detección de intrusiones (IDS) y los registros de auditoría se utilizan para supervisar las infracciones de control de acceso.

Las listas de control de acceso (ACL) son un método de control de acceso. No se pueden utilizar para supervisar las infracciones.

Las copias de seguridad son un método utilizado para compensar las infracciones de acceso porque le permiten recuperar sus datos. Otras medidas compensatorias incluyen la planificación de la continuidad de las actividades y los seguros.

Objetivo:
Operaciones de seguridad

Subobsecución:
Llevar a cabo actividades de registro y vigilancia

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, auditoría y revisión

---

Pregunta #6 de 163

Id. de pregunta: 1105413

Las pruebas deben ser legalmente permisibles en un tribunal de justicia y deben proporcionar una base para un caso. Todas las siguientes características de la evidencia son importantes, EXCEPTO:

✗ **A)** suficiencia
✗ **B)** Relevancia
✓ **C)** confidencialidad
✗ **D)** fiabilidad

Explicación

Las pruebas no deben ser confidenciales para garantizar que sean legalmente permisibles en un tribunal de justicia. La mayoría de las pruebas no son confidenciales.

Las pruebas deben ser suficientes, confiables y relevantes para garantizar que sean legalmente permisibles en un tribunal de justicia. Para ser suficientes, las pruebas deben convencer a una persona razonable de su validez. Para ser confiables, las pruebas deben ser consistentes con los hechos del caso. Para ser relevante, la evidencia debe tener una relación con los hallazgos.

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender los requisitos para los tipos de investigación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, cinco reglas de evidencia

---

Pregunta #7 de 163

Id. de pregunta: 1105521

¿Qué estipulación generalmente NO se proporciona en un contrato de proveedor fuera del sitio?

✗ **A)** Probar la disponibilidad de la instalación fuera del sitio

✗ **B)** plazo de disponibilidad de la instalación fuera del sitio

✗ **C)** disponibilidad del sitio de la instalación fuera del sitio

✓ **D)** ubicación específica de la instalación fuera del sitio

✗ **E)** costo de la instalación fuera del sitio

Explicación

Un contrato de proveedor fuera del sitio no suele incluir la ubicación específica de la instalación fuera del sitio. Si bien la mayoría de los contratos generalmente prometen proporcionar servicios dentro de la configuración regional de la empresa que necesita el servicio, no se prometen sitios específicos.

Un contrato de proveedor fuera del sitio generalmente incluye la disponibilidad del sitio (qué tan rápido puede estar en funcionamiento el sitio), la disponibilidad de las pruebas (si y cuándo se pueden realizar las pruebas), el costo y el período de disponibilidad (cuánto tiempo se puede usar el sitio en caso de emergencia).

Objetivo:
Operaciones de seguridad

Subobsecución:
Implementar procesos de recuperación ante desastres (DR)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, recuperación y estrategias de múltiples sitios

---

Pregunta #8 de 163

Id. de pregunta: 1114780

¿Qué afirmación es cierta para el manejo de incidentes informáticos?

✗ **A)** El equipo de respuesta a incidentes informáticos es responsable de la recuperación de un sistema.

✓ **B)** En la investigación por parte del equipo de respuesta a incidentes informáticos debe participar un representante de la alta dirección.

✗ **C)** El desarrollo del sistema se puede llevar a cabo mientras se maneja un incidente informático.

✗ **D)** Los daños en un sistema después de que se produce un ataque se pueden reparar mientras se maneja un incidente informático.

Explicación

El equipo de respuesta a incidentes que maneja un incidente informático debe involucrar a representantes de la alta gerencia, el departamento de tecnología de la información, el departamento legal y el departamento de recursos humanos. El equipo central de respuesta a incidentes debe tener conocimientos técnicos sólidos y debe seguir procedimientos estándar y formales para el manejo de incidentes. Los procedimientos de gestión de incidentes deben utilizarse para prevenir daños futuros por incidentes. Deben proporcionar la capacidad de responder rápida y eficazmente a un incidente. La capacidad de gestión de incidentes de la organización debe utilizarse para contener y reparar los daños causados por incidentes. El manejo de incidentes mejora las comunicaciones internas y la preparación de la organización para responder a los incidentes. Ayuda a una organización a prevenir daños en el futuro

Incidentes.

El desarrollo del sistema no debe realizarse mientras se maneja un incidente informático. La copia de seguridad del sistema y el proceso de gestión de riesgos pueden producirse mientras se gestiona un incidente informático.

El propósito principal de un equipo de respuesta a incidentes es responder a incidentes. El equipo de respuesta a incidentes no se centra en el desarrollo y la recuperación de los sistemas. El equipo de recuperación se centra en la recuperación de los sistemas. El departamento de TI generalmente se encarga del desarrollo del sistema.

El daño causado a un sistema informático por un ataque no debe deshacerse durante el manejo de incidentes informáticos. Al seleccionar a los miembros del equipo principal de respuesta a incidentes, se deben tener en cuenta las habilidades de comunicación, el conocimiento técnico y el conocimiento de la política empresarial. Los siguientes puntos están en la agenda del equipo de respuesta a incidentes mientras se investiga un incidente:

- Puntos de contacto e informes fuera de la empresa
- Puntos de contacto para la ciencia forense del sistema
- Proceso utilizado para buscar y asegurar la evidencia, incluidos los miembros del equipo de búsqueda e incautación
- Contenido y formato del informe que se presentará a la administración
- Métodos para tratar con diferentes tipos de sistemas

Después de responder a un incidente, se debe celebrar una reunión dentro de una semana para discutir la intrusión y su investigación. El análisis debería resultar útil para prevenir futuros ataques y mejorar los procedimientos de respuesta de emergencia.

El personal de capacitación en seguridad tiene una mejor comprensión del conocimiento de los usuarios sobre los problemas de seguridad. Los entrenadores pueden utilizar incidentes reales para ilustrar vívidamente la importancia de la seguridad informática. La capacitación que se basa en las amenazas y controles actuales recomendados por el personal de manejo de incidentes proporciona a los usuarios información más específicamente dirigida a sus necesidades actuales, lo que reduce los riesgos de incidentes para la organización.

Objetivo:

Operaciones de seguridad

Subobsecución: Llevar

a cabo la gestión de incidentes

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, gestión de respuesta a incidentes

---

Pregunta #9 de 163

Id. de pregunta: 1105489

¿Qué afirmación es cierta de una base informática de confianza (TCB)?

- ✗ **A)** Un TCB garantiza que un sistema informático sea completamente seguro en todo momento.
- ✗ **B)** Un TCB sólo direcciona el sistema operativo de un equipo.
- ✗ **C)** El término TCB se originó a partir de las normas ITSEC.
- ✓ **D)** Un TCB contiene el núcleo de seguridad y otros mecanismos de protección de seguridad.

Explicación

Una base informática de confianza (TCB) contiene el núcleo de seguridad y otros mecanismos de protección de seguridad. Los componentes del kernel de seguridad desempeñan un papel en la aplicación de la directiva de seguridad del equipo mediante la aplicación del monitor de referencia. La ruta de acceso segura entre un usuario y trusted computing base (TCB) se denomina ruta de acceso de confianza.

El término TCB no se originó en las normas ITSEC. Se originó a partir del Libro Naranja o TCSEC.

Un TCB aborda el hardware, el firmware y el software de un sistema informático, no solo el sistema operativo del equipo.

La evaluación del TCB asegura que el sistema actuará de manera predecible y consistente. El proceso de evaluación detallado se vuelve más fácil si el tamaño del TCB es pequeño. Un TCB no puede garantizar que un sistema informático sea completamente seguro en todo momento.

El TCB se refiere a los mecanismos y componentes de protección dentro de un sistema que aplica la directiva de seguridad. El TCB aborda el nivel de confianza que proporciona un sistema en lugar del nivel de seguridad. El límite que separa el TCB del resto del sistema se denomina perímetro de seguridad.

Objetivo:
Operaciones de seguridad

Subobsecución:
Operar y mantener medidas detectivescas y preventivas

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, recuperación de confianza

---

Pregunta #10 de 163

Id. de pregunta: 1192961

Los usuarios informan de que el servidor de Terminal Server de Windows Server de su empresa está experimentando problemas de rendimiento. Tiene una línea de base de rendimiento para el servidor. Sospecha que el servidor de Terminal Server está bajo ataque de un pirata informático. ¿Qué herramienta debe utilizar para determinar si el rendimiento del servidor se ha degradado?

- ✗ **A)** un escáner de puertos
- ✗ **B)** una prueba de vulnerabilidad
- ✗ **C)** un analizador de red
- ✓ **D)** Monitor de sistema

Explicación

Debe utilizar el Monitor de sistema para determinar si el rendimiento del servidor se ha degradado. El Monitor de sistema puede supervisar determinados contadores. Estas estadísticas de contador se pueden comparar con la línea base de rendimiento original para determinar si se ha producido una degradación del rendimiento. Antes de Windows 2000, el Monitor de rendimiento proporcionaba esta información. En Windows 2000, el Monitor de sistema reemplazó al Monitor de rendimiento.

No debe utilizar un escáner de puertos. Un escáner de puertos proporcionará información sobre los puertos y servicios que están disponibles en la red.

No debe utilizar un analizador de red. Un analizador de red puede proporcionar información estadística de red, pero no puede proporcionar información de rendimiento para un único equipo.

No debe utilizar una prueba de vulnerabilidad. Una prueba de vulnerabilidad comprueba la red en busca de vulnerabilidades conocidas y proporciona métodos de protección contra las vulnerabilidades.

Objetivo:
Operaciones de seguridad

Subobsecución:

Llevar a cabo actividades de registro y vigilancia

Referencias:

Utilizar el Monitor de rendimiento de Windows para establecer una línea base de un servidor Terminal Server (parte 1), HYPERLINK "http://techgenix.com/windows-performance-monitor-baseline-terminal-server-part2/" \t "sean" http://www.msterminalservices.org/articles/Windows-Performance-Monitor-Baseline-Terminal-Server-Part1.html

---

Pregunta #11 de 163

Id. de pregunta: 1105498

¿Cuál es una descripción correcta de un sistema honeypot?

- ✓ **A)** Un equipo utilizado para atraer a un atacante
- ✗ **B)** Una herramienta utilizada para detectar alteraciones en los archivos de sistema
- ✗ **C)** una metodología de prueba utilizada para revelar vulnerabilidades
- ✗ **D)** Un tipo de ataque en el que el sistema de destino está inundado de solicitudes de servicio no autorizadas

Explicación

Se instala un sistema honeypot para atraer a posibles atacantes. Un sistema honeypot se instala generalmente junto con los servicios populares y los puertos habilitados detrás de un firewall en una zona desmilitarizada (DMZ). Este sistema debe aislarse para evitar que obstaculice el funcionamiento de una red protegida. La implementación de este sistema subraya la diferencia entre los conceptos de atrapamiento y seducción. El atrapamiento se refiere a inducir a un intruso a cometer un crimen no deseado. Seducción se refiere al proceso de hacer que un equipo vulnerable a los ataques mediante la creación de puertos y servicios populares disponibles en el equipo.

Un comprobador de integridad de archivos es una herramienta que se utiliza para determinar si los atacantes han modificado algún archivo. Normalmente, alterarán los registros de eventos y aplicaciones de un equipo o los archivos críticos del sistema. Un comprobador de integridad de archivos permite un análisis rápido de un archivo para ver si ha cambiado de alguna manera. Cuando la seguridad se ve comprometida, un atacante a menudo altera ciertos archivos clave para proporcionar acceso continuo y evitar la detección. En primer lugar, se aplica un hash de resumen de mensaje a los archivos de clave en la creación inicial del sistema. Más adelante, puede comprobar los archivos periódicamente para asegurarse de que el archivo no se ha modificado.

Las pruebas de penetración se utilizan para evaluar la capacidad de un sistema para resistir un ataque y revelar cualquier vulnerabilidad del sistema o de la red. Las pruebas de penetración, que también se denominan hacking ético, son el procedimiento de evaluación de vulnerabilidades que realizan los profesionales de la seguridad después de recibir la aprobación de la dirección. Las pruebas de penetración son el proceso en el que los expertos en seguridad utilizan herramientas de seguridad para identificar las vulnerabilidades del sistema. Los hackers éticos utilizan

herramientas que tienen el potencial de evaluar fallas de seguridad sin explotar las vulnerabilidades en la infraestructura de red de una organización. El objetivo principal de las pruebas de penetración o hacking ético es evaluar la capacidad del sistema para resistir ataques y revelar vulnerabilidades del sistema y de la red. Ejemplos de pruebas de penetración incluyen marcación de guerra, olfato y escaneo.

En un ataque de denegación de servicio (DoS), el equipo de destino se inunda con solicitudes de servicio no autorizadas. En este tipo de ataque, un atacante inunda los equipos de destino con varias solicitudes de servicio hasta que se que se quedas sin recursos y hacen que el equipo se congele o se bloquee.

Objetivo:
Operaciones de seguridad

Subobsecución:
Operar y mantener medidas detectivescas y preventivas

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 4: Comunicación y Seguridad de la Red, Honeypot

---

Pregunta #12 de 163

Id. de pregunta: 1105406

Usted es el investigador de incidentes de su organización que realiza una investigación de incidentes de rutina. El siguiente paso que debe realizar es el análisis de red. ¿Cuál de los siguientes ejemplos se considera este tipo de análisis?

- ✗ **A)** análisis de contenido
- ✗ **B)** imágenes de disco
- ✓ **C)** análisis de registros
- ✗ **D)** ingeniería inversa

Explicación

El análisis de registros es un ejemplo de un análisis de red. El análisis de red incluye análisis de comunicaciones, análisis de registros y seguimiento de rutas.

Las otras opciones no son ejemplos de análisis de red.

La ingeniería inversa es un ejemplo de análisis de software. Otros ejemplos de análisis de software incluyen la revisión de código malicioso y la revisión de vulnerabilidades.

El análisis de contenido y las imágenes de disco son ejemplos de análisis de medios. Otros ejemplos de análisis de medios incluyen modificar, acceder, crear (MAC) análisis de tiempo, análisis de espacio de holgura y esteganografía.

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender y apoyar las investigaciones

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, análisis de red

---

Pregunta #13 de 163

Id. de pregunta: 1105454

Su organización ha decidido implementar una columna vertebral dual. ¿Cuál es el propósito de esto?

- ✗ **A)** Para proporcionar redundancia de controlador de disco duro
- ✗ **B)** Para proporcionar redundancia de disco duro
- ✗ **C)** Para proporcionar redundancia de servidor
- ✓ **D)** para proporcionar redundancia de red de área local (LAN)

Explicación

El propósito de una estructura básica dual es proporcionar redundancia de red de área local (LAN). Tal configuración permite que la red funcione en caso de que el cableado principal de LAN no esté operativo.

La redundancia de disco duro se proporciona normalmente mediante el sombreado de disco, la duplicación de disco u otras implementaciones de matriz redundante de disco independiente (RAID).

La redundancia de servidor normalmente la proporcionan los servidores redundantes o de agrupación en clústeres. La agrupación en clústeres configura varios equipos juntos para formar una granja de servidores, donde cada servidor está operativo. En el caso de que uno de los servidores se desespere, los demás servidores seguirán funcionando. Un clúster de servidores aparece al usuario como un único servidor. En una configuración de servidor redundante, el servidor de copia de seguridad está sin conexión hasta que el servidor principal no está operativo.

La redundancia del controlador de disco duro se proporciona mediante la duplicación de disco. La duplicación de disco también proporciona redundancia de disco duro.

Objetivo:
Operaciones de seguridad

Subobsecución:
aprovisionamiento seguro de recursos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, redundancia y tolerancia a fallos

Columna vertebral, http://www.certiguide.com/netplus/cg_np_GlossaryB.htm

¿Qué es una columna vertebral?, http://www.webopedia.com/TERM/b/backbone.html

---

Pregunta #14 de 163

Id. de pregunta: 1105493

Su empresa ha implementado un sistema de detección de intrusiones basado en host (HIDS). Recientemente se ha preocupado por los problemas cuando se implementan estos sistemas. ¿Cuál es un problema importante al implementar este tipo de sistema?

- ✗ **A)** Normalmente se ejecuta como un servicio o un proceso en segundo plano.
- ✗ **B)** Se supervisa todo el tráfico de red entrante al host.
- ✓ **C)** Debe implementarse en cada equipo que lo necesite.
- ✗ **D)** Es difícil descubrir los archivos que han sido alterados por un ataque.

Explicación

Un problema importante al implementar un HIDS es que debe implementarse en cada equipo que lo necesite. Debido a que el HIDS está instalado en el equipo local, el equipo se ve completamente comprometido una vez que un hacker penetra en el software HIDS.

Con un HIDS, es fácil descubrir los archivos que han sido alterados por un ataque. Esto se debe a que un HIDS puede potencialmente mantener sumas de comprobación en los archivos.

Un HIDS no supervisa todo el tráfico de red entrante al host. Un HIDS examina los registros del equipo, los eventos del sistema y los eventos de aplicación. Las capacidades de detección de un HIDS están limitadas por el ámbito de los registros de auditoría.

Un HIDS normalmente se ejecuta como un servicio o proceso en segundo plano, pero esto no se considera un problema importante.

Objetivo:
Operaciones de seguridad

Subobsecución:
Operar y mantener medidas detectivescas y preventivas

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Ids de comunicación y seguridad de red

Pregunta #15 de 163

Id. de pregunta: 1114004

Un técnico de seguridad le informa de que un servidor de archivos está experimentando cargas de programa iniciales (IPL) no programadas. ¿Qué declaración explica MEJOR este problema?

✗ **A)** El sistema está arrancando en modo de restauración del sistema.

✗ **B)** El sistema está arrancando en la última configuración válida conocida.

✓ **C)** El sistema se está reiniciando.

✗ **D)** El sistema está arrancando en modo de usuario único.

Explicación

Si un servidor de archivos está experimentando cargas de programa iniciales (IPL) no programadas, el sistema se está reiniciando.

Una IPL no arranca en modo de usuario único. El modo de usuario único permitirá a un administrador realizar funciones administrativas que requieran que ningún usuario remoto tenga acceso al equipo.

Una IPL no arranca en la última configuración válida conocida. Este modo es un modo de Windows que permite a los administradores restaurar un equipo a su último estado de arranque conocido. Es especialmente útil cuando los controladores recién instalados no funcionan correctamente.

Una IPL no arranca en modo de restauración del sistema. El modo de restauración del sistema permitirá a un administrador restaurar un equipo a un estado guardado anteriormente.

Objetivo:
Operaciones de seguridad

Subobsecución:
Implementar estrategias de recuperación

Referencias:

IPL - carga inicial del programa, https://www.webopedia.com/TERM/I/IPL.html

Pregunta #16 de 163

Id. de pregunta: 1105421

Después de una reciente violación de seguridad de la red, reunió pruebas informáticas para usar para procesar a los sospechosos. ¿Qué condición debe cumplirse para que las pruebas sean admisibles en un tribunal de justicia?

✗ **A)** El contenido de las pruebas informáticas siempre debe ser verificado por un experto en un tribunal de justicia.

✗ **B)** La relevancia de la evidencia informática no es una preocupación primordial.

✓ **C)** Las pruebas informáticas deben ser suficientes y fiables.

✗ **D)** La evidencia informática debe ser descifrada antes de ser presentada en un tribunal de justicia.

Explicación

Las pruebas informáticas deben ser suficientes y fiables para que sean admisibles ante los tribunales de justicia. Suficiente evidencia informática implica que no hay contradicción de opinión por dos individuos en el análisis de la evidencia informática y que los resultados de los hallazgos de los dos individuos son siempre los mismos. Suficiente evidencia informática prueba la validez de los hallazgos al llegar siempre a la misma conclusión. Por lo tanto, las pruebas informáticas recopiladas de una fuente poco fiable o de una persona no pueden presentarse ante el tribunal de justicia.

Las pruebas informáticas deben ser fácticas y no circunstanciales para establecer un hecho en un tribunal de justicia. Una copia original de un contrato actúa como evidencia informática confiable porque es la prueba de primera mano de la transacción. No se pueden contradecir las pruebas informáticas fiables.

La relevancia de la evidencia informática es tan importante como la fiabilidad y suficiencia de la evidencia informática. Las pruebas informáticas pertinentes se correlacionan razonable y lógicamente con la cuestión que se examina.

A menos que se requiera específicamente, los datos se pueden presentar en la misma forma en que se recopilaron del sitio. No hay necesidad de cifrar la evidencia informática en el momento de la recopilación y descifrarla cuando se presenta en un tribunal de justicia.

El contenido de las pruebas informáticas no necesita ser verificado por un experto en un tribunal de justicia. Si la autenticidad y la fiabilidad de la evidencia informática son cuestionables, se puede utilizar un experto para apoyar la evidencia informática. El experto o un especialista también puede ser utilizado para probar un punto técnico o para proporcionar una opinión.

La cadena de custodia de la evidencia debe mostrar quién reunió, aseguró, administró, manejó, transportó y manipuló la evidencia.

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender los requisitos para los tipos de investigación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, cinco reglas de evidencia

---

Pregunta #17 de 163

Id. de pregunta: 1111768

Como parte de una investigación de incidentes, debe asegurarse de que la copia principal del medio original se almacena correctamente. Se deben completar todos los pasos siguientes, EXCEPTO:

✗ **A)** Selle la copia principal en un contenedor y etiquete el contenedor para asegurarse de que la copia principal es segura.

✗ **B)** Etiquete la copia principal con la fecha, la hora, las iniciales del recopilador y el número de caso, si corresponde.

✓ **C)** Cifre la copia principal para asegurarse de que el contenido está protegido.

✗ **D)** Selle el contenedor con cinta de evidencia y escriba en la cinta para asegurarse de que se pueda detectar un sello roto.

Explicación

No debe cifrar la copia principal para asegurarse de que el contenido está protegido. El cifrado no es necesario. Los datos deben conservarse únicamente en su forma original.

Para asegurarse de que la copia principal del medio original se almacena correctamente, debe completar los pasos siguientes:

- Etiquete la copia principal con la fecha, la hora, las iniciales del recopilador y el número de caso, si corresponde.
- Selle la copia principal en un contenedor contenido y etiquete el contenedor para asegurarse de que la copia principal es segura.
- Selle el contenedor con cinta de evidencia y escriba en la cinta para asegurarse de que se pueda detectar un sello roto.

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender y apoyar las investigaciones

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, análisis de medios

---

Pregunta #18 de 163

Id. de pregunta: 1114790

Debe documentar las directrices adecuadas que deben incluirse como parte de cualquier directiva de seguridad que implique al personal que viaja con dispositivos emitidos por la compañía. Se le ha dado una lista que debe incluirse en las directrices de la siguiente manera:

A. Dispositivos de transporte en equipaje facturado.

B. Utilice el cifrado cuando sea posible.

C. No deje el dispositivo desatendido.

D. No utilice redes WiFi.

¿Cuáles son las directrices válidas que deben incluirse como parte de las directrices para el personal?

- ✓ **A)** Sólo B, C y D
- ✗ **B)** Todas las directrices
- ✗ **C)** Sólo B y C
- ✗ **D)** Sólo A, B y C

Explicación

Deben incluirse las siguientes directrices:

- Utilice el cifrado cuando sea posible.
- No deje el dispositivo desatendido.
- No utilice redes WiFi.

Cuando transporte dispositivos, debe EVITAR el transporte de los dispositivos en el equipaje facturado.

Objetivo:
Operaciones de seguridad

Subobsecución:
Abordar las preocupaciones de seguridad y protección del personal

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, viajes

---

Pregunta #19 de 163

Id. de pregunta: 1105494

Durante una auditoría de seguridad reciente de la red de su empresa, los contratistas sugirieron que los sistemas operativos de los equipos cliente no están suficientemente reforzados. ¿Qué pasos son cruciales para garantizar que un sistema operativo esté reforzado?

✗ **A)** Configure todas las cuentas de usuario adecuadas.

✗ **B)** Instale el software de monitoreo adecuado.

✓ **C)** Deshabilite los servicios innecesarios.

✗ **D)** Instale las herramientas administrativas adecuadas.

Explicación

Para asegurarse de que un sistema operativo está protegido, debe deshabilitar todos los servicios innecesarios y quitar todas las aplicaciones innecesarias.

La instalación de las herramientas administrativas adecuadas y la configuración de las cuentas de usuario adecuadas, aunque es necesaria para el funcionamiento general, no forma parte del proceso de protección.

La instalación de un software de supervisión adecuado, si bien es una buena idea para la seguridad y el rendimiento general, no forma parte del proceso de endurecimiento.

La mayoría de las instalaciones de sistemas operativos lista para usar deben reforzarse para garantizar el cumplimiento de la política de seguridad de su empresa. Al proteger un sistema operativo, también debe asegurarse de que cualquier cuenta administrativa o raíz tenga la contraseña y los privilegios adecuados. También debe asegurarse de que todas las características de seguridad están configuradas para cumplir con la directiva de seguridad de su empresa. También es necesario segregar las comunicaciones entre procesos.

Objetivo:
Operaciones de seguridad

Subobsecución:
Operar y mantener medidas detectivescas y preventivas

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 7: Operaciones de seguridad, endurecimiento del sistema

---

Pregunta #20 de 163

Id. de pregunta: 1105462

Los usuarios informan de que tienen problemas para acceder a varios servidores de la red de la organización. La causa de este problema debe ser determinada. ¿Quién debe solucionar este problema?

✗ **A)** equipo de continuidad del negocio

✓ **B)** equipo de operaciones

✗ **C)** administrador del servidor

✗ **D)** administrador de red

Explicación

El equipo de operaciones debe determinar la causa de este problema. El equipo de operaciones es responsable de prevenir problemas, reducir los errores de hardware y software y reducir el impacto de los incidentes.

Dado que hay varios servidores implicados, el administrador del servidor no sería la mejor persona para solucionar este problema. Sin embargo, el administrador del servidor puede incluirse como miembro del equipo de operaciones para asegurarse de que se utiliza la experiencia del administrador.

Dado que el problema se está produciendo con varios servidores en la red, el administrador de red no sería la mejor persona para solucionar este problema. Sin embargo, el administrador de red puede incluirse como miembro del equipo de operaciones para asegurarse de que se utiliza la experiencia del administrador.

El equipo de continuidad del negocio es responsable de desarrollar el plan de continuidad del negocio, incluida la realización del análisis de impacto del negocio (BIA), el desarrollo de un plan de contingencia y el mantenimiento del plan de continuidad del negocio (BCP).

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender y aplicar conceptos fundamentales de operaciones de seguridad

Referencias:

CISSP Cert Guide (3ª edición),Capítulo 1: Seguridad y gestión de riesgos, recuperación de datos

---

Pregunta #21 de 163

Id. de pregunta: 1105551

¿Qué afirmación es cierta de la iluminación de áreas críticas?

✗ **A)** Las áreas críticas deben usar iluminación de emergencia y estar iluminadas de seis pies de altura a dos pies-velas.

✗ **B)** Las áreas críticas deben usar iluminación de viaje y estar iluminadas de diez pies de altura a cuatro velas de pie.

✓ **C)** Las áreas críticas deben usar iluminación continua y estar iluminadas de ocho pies de altura a dos velas de pie.

✗ **D)** Las áreas críticas deben usar iluminación de reserva y estar iluminadas de diez pies de altura a dos velas de pie.

Explicación

De acuerdo con las directrices del Instituto Nacional de Estándares y Tecnología (NIST) relativas a la protección perimetral, las áreas críticas deben iluminarse de ocho pies de altura a dos velas de iluminación (21.528 lux). Las velas de pie son una unidad para medir la intensidad de la luz dentro de una esfera de un pie que rodea la fuente de luz. Para la iluminación de áreas críticas, debe haber una distancia adecuada entre los accesorios para proteger una instalación contra posibles intrusos. Las áreas críticas deben iluminarse con iluminación ininterrumpida que consiste en una serie de luminarias fijas, como iluminaciones de proyección de deslumbramiento, que iluminan las áreas oscuras circundantes. La iluminación perimetral, incluida la iluminación para estacionamientos y entradas, debe instalarse para desalentar a los merodeadores o intrusos ocasionales.

La iluminación de disparo implica el uso de sensores que activan la luz cuando cualquier intruso cruza un punto de activación. La iluminación de viaje se puede utilizar para iluminar áreas críticas, pero generalmente se prefiere la iluminación continua.

La iluminación en espera no es continua y difiere de la iluminación continua en que la iluminación en espera se activa de forma automática o manual si hay alguna actividad sospechosa.

La iluminación de emergencia se utiliza durante cortes de energía u otras emergencias que interrumpen las actividades normales del sistema. Esta opción también es incorrecta porque no sigue los estándares del NIST con respecto a la iluminación de áreas críticas.

El área iluminada por una luminaria de poste depende de la potencia de las bombillas y la altura del poste. Cuanto mayor sea la potencia de las bombillas, mayor será el área iluminada. Para la seguridad perimetral, el área iluminada por cada luminaria de poste de luz debe superponerse. Por ejemplo, si las bombillas pueden proporcionar iluminar un radio de 20 pies, los postes de luz deben erigirse a menos de 20 pies de distancia para que la luz se superponga.

Objetivo:
Operaciones de seguridad

Subobjetiva:
Implementar y administrar la seguridad física

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 7: Operaciones de Seguridad, Iluminación

Pregunta #22 de 163

Id. de pregunta: 1114005

¿Cuál es el término para RAID 1 implementado con un solo controlador de disco duro?

- ✗ **A)** creación de bandas de disco
- ✗ **B)** duplicación de disco
- ✗ **C)** creación de bandas de disco con paridad
- ✓ **D)** espejado de disco

Explicación

Matriz redundante de discos independientes (RAID) 1 implementada con un único controlador de disco duro se conoce como duplicación de disco. Con la creación de reflejo de disco, dos discos duros están conectados a la misma controladora de disco duro y se almacena una copia completa de cada archivo en cada disco duro.

La duplicación de discos también es una implementación de RAID 1. Sin embargo, con la duplicación de disco, cada disco duro está conectado a un controlador de disco duro independiente. El uso de controladores de disco duro independientes proporciona una mayor tolerancia a errores. Como regla general, la tolerancia a errores significa que un sistema es capaz de detectar y corregir un error.

La creación de bandas de disco es RAID 0. Los archivos de una matriz RAID 0 se almacenan en bandas, que son pequeños bloques de datos. Es posible que partes de un archivo grande se almacenen en todos los discos de una matriz RAID 0.

RAID 5 es la creación de bandas de disco con paridad. Una franja almacenada en una matriz RAID 5 es una franja de paridad. Los datos almacenados en cualquier disco de una matriz RAID 5 se pueden reconstruir a partir de las bandas de paridad almacenadas en los otros discos de la matriz. Debido a que RAID 5 utiliza la paridad para proporcionar tolerancia a errores a través de la matriz, un disco en él puede dañarse y, por lo general, puede simplemente sacarlo sin apagar el sistema (intercambio en caliente) y conectar un disco de repuesto en la bahía. A continuación, la matriz comenzará automáticamente a reconstruir la información del nuevo disco con la paridad contenida a través de los otros discos de la matriz. Esta capacidad de intercambio en caliente suele estar presente en servidores empresariales que requieren alta disponibilidad.

Objetivo:
Operaciones de seguridad

Subobsecución:
Implementar estrategias de recuperación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 2: Seguridad de activos: RAID

Pregunta #23 de 163

Id. de pregunta: 1105552

¿Qué opción NO es un control administrativo para la seguridad física?

- ✗ **A)** gestión de instalaciones
- ✗ **B)** control de personal
- ✓ **C)** detección de intrusiones
- ✗ **D)** respuesta y procedimientos de emergencia

Explicación

La detección de intrusiones es un ejemplo de controles técnicos y no de controles administrativos. La detección de intrusiones, alarmas, CCTV, detección de incendios y supresión son algunos ejemplos de controles técnicos.

La respuesta y los procedimientos de emergencia, los controles de personal y la administración de instalaciones son algunos ejemplos de controles administrativos utilizados para mantener la seguridad física de una instalación.

Objetivo:
Operaciones de seguridad

Subobjetiva:
Implementar y administrar la seguridad física

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, Administrativa (Gestión)

Pregunta #24 de 163

Id. de pregunta: 1105424

Se ha producido una infracción de seguridad en el servidor de archivos de su organización. Como parte de una investigación de incidentes, se han creado dos copias de los medios originales. Se le ha pedido que cree resúmenes de mensajes para los archivos y directorios en el medio antes de que se analicen los datos.

¿Cuál es el propósito de esta acción?

- ✗ **A)** para probar la confidencialidad de la imagen original
- ✗ **B)** Para asegurarse de que el medio antiguo no contiene datos residuales
- ✓ **C)** para demostrar la integridad de la imagen original
- ✗ **D)** Para asegurarse de que el nuevo medio no contiene datos residuales

Explicación

Al crear resúmenes de mensaje para los archivos y directorios, los resúmenes de mensaje se utilizan para demostrar la integridad de la imagen original. Si los resúmenes del mensaje no han cambiado, los datos originales no se han cambiado.

La purga garantiza que los medios no contengan datos residuales. Purgar nuevos medios antes de usarlos para almacenar una copia de datos es importante.

Para proporcionar confidencialidad de una imagen, tendría que cifrar la imagen.

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender los requisitos para los tipos de investigación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, preservar y recopilar evidencia

---

Pregunta #25 de 163

Id. de pregunta: 1105495

Su empresa implementa un honeypot como prevención de intrusiones. A la gerencia le preocupa que este honeypot se considere atrapamiento y le ha pedido que se asegure de que no se produzca el atrapamiento. ¿Qué situación debes prevenir?

- ✗ **A)** permitir la navegación web en un honeypot
- ✓ **B)** permitir descargas en un honeypot
- ✗ **C)** puertos abiertos en un honeypot
- ✗ **D)** servicios abiertos en un honeypot

Explicación

Debe evitar permitir descargas en un honeypot. Permitir descargas en un honeypot es un posible ejemplo de atrapamiento si se utiliza para hacer cargos formales de allanamiento de morada. El atrapamiento se produce cuando un hacker es engañado para que realice una actividad ilegal. El atrapamiento de trampas es ilegal.

Abrir el puerto y los servicios y permitir la navegación web en un honeypot no son ejemplos de atrapamientos. Son tentaciones. La tentación permite al administrador supervisar la actividad para aumentar la seguridad y quizás rastrear el ataque. La tentación es legal.

Objetivo:
Operaciones de seguridad

Subobsecución:
Operar y mantener medidas detectivescas y preventivas

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y Seguridad de Red Honeypot

---

Pregunta #26 de 163

Id. de pregunta: 1105520

¿Qué ocurre durante la fase de reconstitución de una recuperación?

- ✓ **A)** Una organización vuelve a su sitio original
- ✗ **B)** Una organización implementa la estrategia de recuperación
- ✗ **C)** Una organización garantiza que sus instalaciones se restauren por completo en el sitio alternativo
- ✗ **D)** Una organización realiza la transición a un sitio alternativo temporal

Explicación

Durante la fase de reconstitución de la recuperación ante desastres, una organización realiza la transición a su sitio original o a un nuevo sitio que se construyó para reemplazar el sitio original. Una organización no se considera completamente restaurada hasta que está operando desde su ubicación original o de reemplazo.

Ninguna de las otras opciones define lo que ocurre durante la fase de reconstitución.

Objetivo:
Operaciones de seguridad

Subobsecución:
Implementar procesos de recuperación ante desastres (DR)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y gestión de riesgos, recuperación ante desastres y el plan de recuperación ante desastres (DRP)

Pregunta #27 de 163

Id. de pregunta: 1114777

Está configurando los equipos servidor para una nueva empresa. Se le ha pedido que diseñe las listas de control de acceso (ACL) para los archivos y carpetas de los servidores. ¿Qué principios afectan al diseño?

un. Kerberos

b. SÉSAMO

c. necesidad de saber

d. Privilegio mínimo

e. inicio de sesión único

- ✗ **A)** opción e
- ✗ **B)** sólo opciones c, d y e
- ✗ **C)** Sólo las opciones A y B
- ✗ **D)** opción c
- ✗ **E)** Opción d
- ✗ **F)** opción A
- ✓ **G)** Sólo las opciones C y D
- ✗ **H)** opción b

Explicación

La necesidad de conocer y los privilegios mínimos afectan al diseño de las listas de control de acceso (ACL). El principio de necesidad de conocer asegura que a los sujetos solo se les dé acceso a los objetos que requieren para completar sus deberes. El principio de privilegios mínimos garantiza que los sujetos reciban el nivel mínimo de permisos de acceso que necesitan para completar sus tareas.

Kerberos y SESAME son dos protocolos de autenticación que afectan al diseño del proceso de autenticación. Ambos protocolos permiten el inicio de sesión único, lo que significa que los usuarios solo inician sesión una vez. Open Group ha definido los siguientes objetivos funcionales para admitir una interfaz de inicio de sesión único (SSO) de usuario:

- La interfaz será independiente del tipo de información de autenticación que se maneje.
- No predefinirá la sincronización de las operaciones de inicio de sesión secundario.
- Se proporcionará apoyo para que un sujeto establezca un perfil de usuario predeterminado.

Al diseñar ACL, debe tener en cuenta que el nivel predeterminado de seguridad debe ser sin acceso. En el diseño de seguridad, lo que no se permite explícitamente debe denegarse implícitamente.

Objetivo:

Operaciones de seguridad

Subobsecución:

aprovisionamiento seguro de recursos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, necesidad de saber / privilegios mínimos

---

Pregunta #28 de 163

Id. de pregunta: 1114009

¿Qué término es una estimación de la cantidad de tiempo que durará un equipo y generalmente es determinado por el proveedor del equipo o un tercero?

- ✗ **A)** BCP
- ✗ **B)** BIA
- ✗ **C)** MTTR
- ✓ **D)** MTBF

Explicación

El tiempo medio entre fallas (MTBF) es una estimación de la cantidad de tiempo que durará un equipo y generalmente lo determina el proveedor del equipo o un tercero.

El tiempo medio de reparación (MTTR) es una estimación de la cantidad de tiempo que se tardará en reparar un equipo y devolverlo a producción. El propietario del equipo generalmente determina esta cantidad de tiempo.

Se crea un análisis de impacto empresarial (BIA) para identificar las funciones vitales y priorizarlas en función de las necesidades. Se identifican las vulnerabilidades y amenazas, y se calculan los riesgos.

Se crea un plan de continuidad del negocio (BCP) para garantizar que se establezcan políticas para hacer frente a las interrupciones y desastres a largo plazo. Su objetivo principal es garantizar que la empresa mantenga sus objetivos comerciales a largo plazo tanto durante como después de la interrupción y se centra principalmente en la continuidad de la infraestructura de datos, telecomunicaciones y sistemas de información.

Los elementos de la aprobación e implementación del plan BCP incluyen:

- Crear una conciencia del plan
- Obtención de la aprobación de los resultados por parte de la alta dirección
- Actualización del plan regularmente y según sea necesario

El BCP debe ser probado si ha habido cambios sustanciales en la empresa o el medio ambiente. También deben hacerse la prueba al menos una vez al año.

Objetivo:

Operaciones de seguridad

Subobsecución:

Participar en la planificación y los ejercicios de continuidad del negocio (BC)

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 7: Operaciones de Seguridad, MTBF y MTTR

Pregunta #29 de 163

Id. de pregunta: 1105444

¿Qué declaración NO es una característica de un sistema de detección de intrusiones (NIDS) basado en red?

- ✗ **A)** Un NIDS no supervisa las estaciones de trabajo individuales en una red.
- ✗ **B)** Un NIDS supervisa el tráfico en tiempo real.
- ✓ **C)** Un NIDS analiza la información cifrada.
- ✗ **D)** Un NIDS analiza los paquetes de red en busca de intrusión.

Explicación

La principal desventaja de un NIDS es su incapacidad para analizar la información cifrada. Por ejemplo, los paquetes que atraviesan a través de un túnel de red privada virtual (VPN) no se pueden analizar por el NIDS.

Un NIDS puede supervisar una red completa o algunas partes de una red segregada. Permanece pasivo mientras adquiere los datos de la red. Por ejemplo, un sistema de detección de intrusiones (IDS) se puede colocar en la red interna para supervisar el tráfico en tiempo real o una zona desmilitarizada (DMZ). En una dmz, los servidores públicos, como los servidores de correo electrónico, DNS y FTP, se hospedan en una organización para segregar estos servidores públicos de la red interna. Un NIDS supervisa el tráfico en tiempo real a través de la red, captura los paquetes y los analiza a través de una base de datos de firmas o contra el comportamiento normal del patrón de tráfico para asegurarse de que no hay intentos de intrusión o amenazas malintencionadas. NIDS encuentra una amplia implementación comercial en la mayoría de las organizaciones.

Un NIDS no supervisa estaciones de trabajo específicas. Un IDS basado en host (HIDS) supervisa las estaciones de trabajo individuales en una red. Se debe instalar un agente de detección de intrusiones en cada estación de trabajo individual de un segmento de red para supervisar cualquier intento de infracción de seguridad en un host.

Objetivo:

Operaciones de seguridad

Subobsecución:

Llevar a cabo actividades de registro y vigilancia

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 4: Comunicación y Seguridad de red, IDS

Pregunta #30 de 163

Id. de pregunta: 1105490

¿Qué tipo de seguridad identifica el proceso de protección de los activos de información después de la implementación de la seguridad?

- ✗ **A)** seguridad de las aplicaciones
- ✗ **B)** seguridad física
- ✓ **C)** seguridad de las operaciones
- ✗ **D)** seguridad de control de acceso

Explicación

El objetivo principal de la seguridad de las operaciones es protegerse contra las amenazas de activos de información generadas dentro de una organización. Incluye tomar medidas para asegurarse de que un entorno y las cosas que lo componen están cubiertos por un cierto nivel de protección. La seguridad de las operaciones es importante porque un entorno cambia continuamente y tiene el potencial de reducir su nivel de protección.

La seguridad de las operaciones tiene como objetivo el mantenimiento continuo de la infraestructura de seguridad a través de la implementación de actividades rutinarias que mantienen la infraestructura en funcionamiento de manera segura. La seguridad de las operaciones también depende de los procedimientos y procesos rutinarios de otros tipos de seguridad. Por ejemplo, para permitir la seguridad de las operaciones, se deben implementar y mantener controles de seguridad físicos, garantizando así la confidencialidad, integridad y disponibilidad de las operaciones empresariales.

Los controles físicos se refieren a la seguridad del perímetro de la instalación, incluyendo cercas, puertas, cerraduras e iluminación. Los controles de seguridad física trabajan en conjunto con la seguridad de la operación para lograr los objetivos de seguridad de la organización.

Los controles de seguridad de aplicaciones proporcionan procesos para la entrada, el procesamiento, las comunicaciones entre procesos, la comunicación entre diferentes programas y la salida resultante.

El control de acceso es un método para limitar el acceso a los recursos a los usuarios autorizados e impedir el acceso a los usuarios ilegítimos.

Objetivo:

Operaciones de seguridad

Subobsecución:

Operar y mantener medidas detectivescas y preventivas

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, activos de información

---

Pregunta #31 de 163

Id. de pregunta: 1114771

Está realizando análisis de dispositivos integrados en un chip GPS en un teléfono móvil. Realizar hash criptográfico, crear sumas de comprobación y documentar toda la evidencia. ¿Qué fase del análisis de dispositivos integrados está realizando?

- ✗ **A)** Colección
- ✗ **B)** Presentación
- ✓ **C)** Preservación
- ✗ **D)** Análisis

Explicación

Está realizando la fase de conservación del análisis de dispositivos incrustados al realizar hash criptográfico, crear sumas de comprobación y documentar toda la evidencia.

Hay siete fases de investigación forense:

1) Identificación

2) Preservación

3) Colección

4) Examen

5) Análisis

6) Presentación

7) Decisión

Objetivo:

Operaciones de seguridad

Subobsecución:
Comprender y apoyar las investigaciones

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, hardware / análisis de dispositivos integrados

---

Pregunta #32 de 163

Id. de pregunta: 1105423

¿A quién se le permite más probablemente dar pruebas de opinión en la corte?

- ✗ **A)** un investigador de incidentes
- ✗ **B)** un testigo
- ✓ **C)** un experto
- ✗ **D)** un oficial de la ley

Explicación

Un experto puede dar pruebas de opinión en la corte. El experto se utiliza para asegurarse de que el juez y el jurado entiendan alguna cuestión del caso. Un experto puede ofrecer una opinión basada en la experiencia personal y los hechos, pero un no experto puede testificar sólo en cuanto a los hechos.

Ninguna de las otras opciones es correcta.

Los testigos no pueden dar testimonio de opinión en la corte. Dan pruebas directas. La evidencia directa prueba o refuta un acto específico a través del testimonio oral basado en la información recopilada a través de los cinco sentidos del testigo.

Es probable que un oficial de la ley no dé evidencia de opinión en la corte a menos que se le pregunte sobre los procedimientos probatorios en los que el oficial es un experto.

Un investigador de incidentes no da evidencia de opinión. Por lo general, dan evidencia secundaria o directa.

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender los requisitos para los tipos de investigación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, evidencia de opinión

---

Pregunta #33 de 163

Id. de pregunta: 1105434

Se le ha pedido que implemente un sistema que detecte los intentos de intrusión en la red y controle el acceso a la red para los intrusos. ¿Qué sistema debe implementar?

✗ **A)** cortafuegos
✗ **B)** IDENTIFICADORES
✗ **C)** VPN
✓ **D)** IPS

Explicación

Un sistema de prevención de intrusiones (IPS) detecta los intentos de intrusión en la red y controla el acceso a la red para los intrusos. Un IPS es una mejora sobre un sistema de detección de intrusiones (IDS) porque un IPS previene realmente la intrusión.

Un firewall es un dispositivo que está configurado para permitir o impedir cierta comunicación basada en filtros preconfigurados. Un cortafuegos puede proteger un equipo o una red de intrusiones no deseadas mediante estos filtros. Sin embargo, cualquier comunicación no definida específicamente en los filtros se permite o se deniega. Los cortafuegos no se utilizan para detectar intrusiones en la red. Sin embargo, los firewalls evitan la comunicación no deseada basada en reglas predefinidas.

Un IDS sólo detecta la intrusión y registra la intrusión o notifica al personal adecuado.

Una red privada virtual (VPN) es una red privada a la que los usuarios pueden conectarse a través de una red pública.

Objetivo:
Operaciones de seguridad

Subobsecución:
Llevar a cabo actividades de registro y vigilancia

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 4: Comunicación y Seguridad de Red, IPS

Pregunta #34 de 163

Id. de pregunta: 1114789

Desea asegurarse de que los empleados pueden utilizar un código para alertar a las autoridades correspondientes cuando están bajo coacción. ¿Con qué medida de seguridad física se puede utilizar?

a. Bloqueo de cifrado

b. Guardia de seguridad

c. bloqueo combinado

d. Sistema biométrico

- ✗ **A)** opción c
- ✗ **B)** opciones b, c y d
- ✗ **C)** opción b
- ✗ **D)** Opción d
- ✓ **E)** opciones a, b y d
- ✗ **F)** opción A
- ✗ **G)** todas las opciones

Explicación

Los códigos de coacción se pueden usar para alertar a las autoridades adecuadas cuando los empleados están bajo coacción cuando se utilizan cerraduras de cifrado y guardias de seguridad. Con un bloqueo de cifrado, el personal utiliza un código para abrir el bloqueo y tiene otro código que deben introducir cuando están bajo coacción. Con los guardias de seguridad, se debe enseñar al personal qué frase o término usar para alertar al guardia de seguridad de que están bajo coacción. Con algunos sistemas biométricos, se puede enseñar al usuario a usar un factor de autenticación diferente (por ejemplo, el segundo dedo en lugar del primer dedo o el ojo derecho en lugar del ojo izquierdo), y el uso del factor incorrecto permitirá el acceso, pero también señalará una alarma de coacción.

Los bloqueos de combinación requieren que se introduzca la combinación adecuada para abrirse. Las cerraduras combinadas no son electrónicas y no se pueden programar para reconocer un código de coacción.

Otra esfera de consideración que las organizaciones deben tener con respecto a la seguridad del personal es la seguridad durante los viajes. Las organizaciones deben proporcionar pautas de seguridad para todos los empleados que viajan. Además, los empleados deben recibir números de emergencia y de emergencia después de la hora para garantizar que puedan alertar a los contactos de la organización.

La privacidad del personal también es una consideración de la organización. Se debe crear una directiva sin expectativas de privacidad para que el personal comprenda el nivel de privacidad que se puede esperar al usar los recursos de la organización. Esta directiva debe indicar explícitamente que se puede supervisar la comunicación. El personal también debe recibir directrices sobre cuáles son los usos aceptables e inaceptables de los recursos de la organización, tal como se define en la Política de uso aceptable.

Objetivo:
Operaciones de seguridad

Subobsecución:

Abordar las preocupaciones de seguridad y protección del personal

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, coacción

---

Pregunta #35 de 163

Id. de pregunta: 1105437

La dirección de la empresa se ha preocupado recientemente por los problemas de seguridad que afectan a los empleados de la empresa. Se le ha pedido que mejore la responsabilidad del usuario mediante la supervisión de eventos del sistema. ¿Qué eventos de auditoría NO deben supervisarse?

✗ **A)** modificaciones de la cuenta

✗ **B)** intentos de inicio de sesión

✓ **C)** creación de archivos

✗ **D)** modificaciones de archivos

Explicación

No es necesario supervisar la creación de archivos. Los usuarios deben poder crear archivos. Cuando un usuario crea un archivo, el nombre de usuario aparece como el propietario del archivo.

Debe supervisar los intentos de inicio de sesión, la modificación de archivos y los eventos de modificación de cuentas para mejorar la responsabilidad del usuario. De acuerdo con el principio de rendición de cuentas, los acontecimientos significativos deben ser rastreables hasta un individuo. Lo que constituye significativo depende de la naturaleza de los datos y de la política de seguridad de la red. Esta responsabilidad individual gira en torno al uso de identificadores únicos, reglas de acceso y pistas de auditoría.

El registro de auditoría es el proceso de realizar un seguimiento de las acciones significativas del usuario. Las acciones que deben ser monitoreadas generalmente son determinadas por la empresa y dependen de las circunstancias comerciales. También debe supervisar los siguientes eventos: uso de utilidades de administración, funciones realizadas y comandos iniciados. Es importante que una empresa determine cuál es su directiva de auditoría para proporcionar la máxima protección y, al mismo tiempo, minimizar el efecto en los recursos del sistema. Al supervisar las transacciones en un registro de auditoría, el registro debe incluir la fecha y hora de la transacción, quién procesó la transacción y en qué terminal se procesó la transacción.

Objetivo:

Operaciones de seguridad

Subobsecución:
Llevar a cabo actividades de registro y vigilancia

Referencias:

HYPERLINK "http://sectools.org/tools2003.html" CISSP Cert Guide (3rd Edition), Chapter 5 Identity and Access Management Auditing and Reporting

---

Pregunta #36 de 163

Id. de pregunta: 1114008

¿Qué plan garantiza que un puesto corporativo vital se llene en caso de que se desocupe durante un desastre?

- ✓ **A)** plan de sucesión ejecutiva
- ✗ **B)** plan de emergencia para ocupantes (OEP)
- ✗ **C)** plan de continuidad de operaciones (COOP)
- ✗ **D)** acuerdo recíproco

Explicación

Un plan de sucesión ejecutiva asegura que un puesto corporativo vital se llene en caso de que sea desocupado durante un desastre. Este plan podría llevarse a cabo en caso de fallecimiento, renuncia o jubilación de un ejecutivo corporativo.

Se crea un plan de emergencia para ocupantes (OEP, por sus, para garantizar que las lesiones y la pérdida de vidas se minimicen cuando se produce una interrupción o un desastre). También se centra en los daños a la propiedad. Las entrevistas no se incluyen como parte de su desarrollo.

Un plan de continuidad de operaciones (COOP) es un documento que explica cómo se mantendrán las operaciones críticas en caso de que ocurra un desastre.

Un acuerdo recíproco es un acuerdo en el que dos compañías acuerdan proporcionar instalaciones fuera del sitio entre sí en caso de que ocurra un desastre.

Objetivo:
Operaciones de seguridad

Subobsecución:
Participar en la planificación y los ejercicios de continuidad del negocio (BC)

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 7: Operaciones de Seguridad, Recursos Humanos

Pregunta #37 de 163

Id. de pregunta: 1192964

A su organización le preocupa que los usuarios no autorizados descarguen datos confidenciales en medios extraíbles. Usted decide cifrar los datos confidenciales de la empresa utilizando la función de cifrado del sistema operativo. ¿Qué garantiza esto?

✗ **A)** Los datos están protegidos dondequiera que residan.

✗ **B)** Los datos están protegidos mientras están en el medio original y en los medios extraíbles.

✗ **C)** Los datos no están protegidos.

✓ **D)** Los datos están protegidos mientras están en el medio original solamente.

Explicación

Cuando se cifran datos confidenciales mediante la característica de cifrado del sistema operativo de un equipo, los datos solo se protegen mientras se encuentra en el medio original. El cifrado se aplica en una sola unidad. Una vez que los datos se copian en otra unidad, el cifrado de archivos ya no se utiliza.

La única manera de proteger los datos confidenciales en el medio extraíble es cifrarlos después de colocarlos en la unidad.

Algunas soluciones de cifrado de terceros proporcionan un medio para proteger varias unidades. Estas soluciones proporcionan cifrado en muchos tipos de dispositivos.

Los medios extraíbles incluyen discos duros extraíbles, unidades flash, discos CD-ROM, unidades USB y cintas. Aunque la mayoría de estos medios se pueden escribir en muchas veces, los discos CD-R son medios de escritura una sola vez. Los discos CD-RW se pueden escribir en varias veces.

Objetivo:
Operaciones de seguridad

Subobjecución:
Aplicar técnicas de protección de recursos

Referencias:

Abordar los riesgos de los medios extraíbles, HYPERLINK "http://www.continuitycentral.com/feature0184.htm" \t "sean" http://www.continuitycentral.com/feature0184.htm

Pregunta #38 de 163

Id. de pregunta: 1105539

¿Qué término se refiere a la cantidad de tiempo que una empresa puede tolerar la interrupción de un determinado activo, entidad o servicio?

- ✓ **A)** tiempo de inactividad máximo tolerable
- ✗ **B)** análisis de impacto en el negocio
- ✗ **C)** tiempo medio entre el error
- ✗ **D)** tiempo máximo de recuperación
- ✗ **E)** tiempo medio de reparación

Explicación

El tiempo de inactividad máximo tolerable (MTD) es la cantidad de tiempo que una empresa puede tolerar la interrupción de un determinado activo, entidad o servicio. El MTD puede variar desde unos pocos minutos hasta unas pocas horas para los activos más críticos hasta 30 días o más para los activos no esenciales. MTD se basa en la criticidad de las operaciones del activo. Por lo general, los activos críticos no se pueden reemplazar mediante métodos manuales. Por ejemplo, un servidor Web que proporciona funciones de comercio electrónico probablemente será más crítico que un servidor de archivos que proporciona una función de almacenamiento para los archivos de los usuarios.

Un análisis de impacto en el negocio (BIA) identifica las operaciones críticas del negocio y calcula el riesgo y las amenazas en las que pueden incurrir esas operaciones.

El tiempo máximo de recuperación es una estimación de la cantidad máxima de tiempo que se tardará en recuperar un sistema. Esta recuperación generalmente incluye la recuperación de copias de seguridad de datos.

El tiempo medio entre fallos (MTBF) es el tiempo estimado que durará un equipo antes de que necesite ser reemplazado. Esto generalmente es proporcionado por el proveedor de equipos.

El tiempo medio de reparación (MTTR) es el tiempo estimado que un equipo estará caído debido a una falla.

Un sistema se considera más fiable cuando tiene un MTBF más alto y un MTTR más bajo.

Objetivo:
Operaciones de seguridad

Subobsecución:
Participar en la planificación y los ejercicios de continuidad del negocio (BC)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y gestión de riesgos, identificar los impactos de las interrupciones y estimar el tiempo de inactividad

Pregunta #39 de 163

Id. de pregunta: 1105426

Ha establecido líneas de base de umbral de error de usuario para la red de su organización que le avisarán si se produce una actividad sospechosa. ¿Cómo se llaman las líneas de base?

✗ **A)** registros de auditoría

✗ **B)** privilegio mínimo

✓ **C)** niveles de recorte

✗ **D)** administración de la configuración

Explicación

Las líneas de base se denominan niveles de recorte. Cuando se supera un nivel de recorte, se registran más infracciones para su revisión. A menudo, el software que detecta la infracción del nivel de recorte enviará una alerta a un administrador de seguridad. Los niveles de recorte ayudan a reducir la cantidad de datos que se evaluarán en los registros de auditoría.

El principio de privilegio mínimo no se está aplicando. Privilegios mínimos significa que un usuario solo debe tener permisos suficientes para completar las tareas de su rol. Al implementar este privilegio, los usuarios que realizan tareas de nivel administrativo solo deben usar sus cuentas de nivel administrativo al realizar esas tareas. Para realizar otras tareas, los usuarios deben usar una cuenta con los permisos mínimos que necesitan para esa tarea. Un ejemplo de uso de privilegios mínimos es la implementación de vistas de base de datos.

La administración de la configuración se implementa para garantizar que los cambios en la seguridad se administran de manera adecuada.

Los registros de auditoría se utilizan para supervisar las actividades del usuario. Los registros de auditoría se pueden utilizar para registrar los errores de usuario o eventos que se producen. Luego, una vez que se superan los niveles de recorte, se generan alertas.

Objetivo:
Operaciones de seguridad

Subobsecución:
Llevar a cabo actividades de registro y vigilancia

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, niveles de recorte

---

Pregunta #40 de 163

Id. de pregunta: 1114788

¿Qué sistema de detección de intrusiones (IDS) utiliza un campo magnético para detectar intrusiones?

- ✓ **A)** un detector de proximidad
- ✗ **B)** un sistema fotoeléctrico
- ✗ **C)** un sistema de detección acústica
- ✗ **D)** un sistema infrarrojo pasivo

Explicación

Un detector de proximidad es un IDS que utiliza un campo magnético o electrostático para detectar intrusiones. Este tipo de IDS también se llama IDS electrostático. El IDS crea un equilibrio

campo electrostático entre sí mismo y el objeto que se está monitoreando. Si un intruso se encuentra dentro de un cierto rango del objeto monitoreado, provoca un cambio de capacitancia. El IDS puede detectar este cambio y hacer sonar una alarma.

Un sistema fotoeléctrico detecta cambios de luz y solo debe usarse en habitaciones sin ventanas. Un sistema infrarrojo pasivo detecta cambios en las olas de calor. Un sistema de detección acústica utiliza micrófonos instalados en toda una habitación para detectar sonido.

Objetivo:
Operaciones de seguridad

Subobjetiva:
Implementar y administrar la seguridad física

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Tipos de cerraduras de puertas

---

Pregunta #41 de 163

Id. de pregunta: 1111765

¿Durante qué paso de la respuesta a incidentes se produce el análisis de causa raíz?

- ✗ **A)** Informes
- ✓ **B)** revisión
- ✗ **C)** detección
- ✗ **D)** recuperación
- ✗ **E)** respuesta

Explicación

El análisis de la causa raíz se produce durante el paso de revisión de la respuesta a incidentes. El análisis de la causa raíz se realiza para asegurarse de que comprende POR QUÉ se produjo un incidente para que pueda evitar que el problema vuelva a ocurrir. Los pasos de respuesta a incidentes son los siguientes:

- Detectar
- Responder
- Mitigar
- Informe
- Recuperar
- Remediar
- Revisión y documento

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender y apoyar las investigaciones

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, procedimientos de respuesta a incidentes

---

Pregunta #42 de 163

Id. de pregunta: 1105447

¿Qué afirmación es cierta de un sistema de detección de intrusiones basado en red (NIDS)?

✗ **A)** Un NIDS está activo mientras se recopilan datos a través de la red.
✓ **B)** Un NIDS no puede detectar un intruso que ha iniciado sesión en un equipo host.
✗ **C)** Un NIDS es finito cuando genera alarmas.
✗ **D)** Un NIDS no analiza la información en tiempo real.

Explicación

Un inconveniente principal de un sistema de detección de intrusiones basado en red (NIDS) es que no puede detectar un ataque a un host si el intruso ha iniciado sesión en el equipo host.

Un NIDS es pasivo cuando adquiere datos a través de la red. Una ventaja principal de NIDS es su uso de información confiable en tiempo real para monitorear la red sin el consumo de muchos recursos.

Objetivo:
Operaciones de seguridad

Subobsecución:
Llevar a cabo actividades de registro y vigilancia

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 4: Comunicación y Seguridad de red, IDS

Pregunta #43 de 163

Id. de pregunta: 1105510

¿Cuál es el término para proporcionar tolerancia a fallos copiando el contenido de un disco duro a otro?

- ✗ **A)** agrupamiento
- ✗ **B)** INCURSIÓN
- ✗ **C)** intercambio en caliente
- ✓ **D)** Espejado

Explicación

La creación de reflejos se produce cuando se proporciona tolerancia a errores copiando el contenido de un disco duro a otro.

La agrupación en clústeres se produce cuando se combinan dos o más servidores que proporcionan el mismo servicio en un clúster. La agrupación en clústeres equilibra la carga entre los servidores o garantiza que si un servidor falla, otro se hace cargo.

El intercambio en caliente es cuando se puede reemplazar una pieza de hardware en un equipo mientras el equipo sigue funcionando.

La matriz redundante de discos independientes (RAID) es una tecnología de disco duro que proporciona tolerancia a fallos y mejora del rendimiento. Si bien algunos niveles de RAID implementan la duplicación, no todos lo hacen.

Objetivo:
Operaciones de seguridad

Subobsecución:
Implementar estrategias de recuperación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 2: Seguridad de activos: RAID

Pregunta #44 de 163

Id. de pregunta: 1111797

¿Qué cubre el último paso de un plan de continuidad del negocio?

✗ **A)** capacitación del personal

✗ **B)** Probar el plan

✗ **C)** analizar los riesgos

✓ **D)** actualizar el plan

Explicación

El último paso de un plan de continuidad del negocio tiene que ver con la actualización del plan. Un plan de continuidad del negocio es un documento vivo que requiere actualizaciones periódicas. Si el plan no se mantiene correctamente, la organización no podrá recuperarse de un desastre.

Probar el plan y capacitar al personal es el siguiente y último paso en el plan de continuidad del negocio. Este paso garantiza que el plan funcione y que el personal entienda cómo implementarlo.

El análisis de riesgos forma parte del Análisis de Impacto empresarial (BIA), que es el segundo paso de un plan de continuidad del negocio.

Los pasos del proceso de planificación de la continuidad del negocio son los siguientes:

- Desarrollar la declaración de política de planificación de la continuidad del negocio.
- Realizar el análisis de impacto empresarial (BIA).
- Identificar controles preventivos.
- Desarrollar las estrategias de recuperación.
- Desarrollar los planes de contingencia.
- Pruebe el plan y capacite a los usuarios.
- Mantener el plan.

Objetivo:
Operaciones de seguridad

Subobsecución:
Probar planes de recuperación ante desastres (DRP)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Planificación de continuidad y el Plan de Continuidad del Negocio (BCP)

Pregunta #45 de 163

Id. de pregunta: 1105468

¿Cuál es el objetivo principal de la gestión de privilegios?

✗ **A)** para garantizar una estructura de presentación de informes adecuada

✗ **B)** Para evaluar la pertenencia a grupos

✗ **C)** Para garantizar la administración de contraseñas

✓ **D)** Para garantizar el control sobre los permisos de usuario y los derechos de acceso

Explicación

La administración de privilegios es el proceso de determinar los requisitos de seguridad de los usuarios, proporcionar autorización de acceso, supervisar los recursos a los que acceden los usuarios y garantizar que los privilegios asignados a los usuarios en forma de permisos y derechos de acceso a los recursos de información de una organización corroboren sus requisitos de trabajo.

El objetivo principal de la administración de privilegios es definir los derechos de los usuarios para acceder a la información de la organización. Las prácticas estándar para una gestión eficaz de privilegios son el uso de los principios de "necesidad de saber" y "privilegio mínimo". El principio de necesidad de saber se basa en la premisa de que a los usuarios se les debe proporcionar acceso a la información que absolutamente requieren para cumplir con sus responsabilidades laborales. Se deniega el acceso a cualquier información adicional a los usuarios que trabajan bajo el principio de privilegios mínimos.

Una pertenencia a un grupo hace referencia a un conjunto de usuarios que comparten derechos de acceso y permisos comunes para realizar una tarea determinada. Por ejemplo, los usuarios que realizan actividades de contabilidad se pueden agrupar en un grupo de contabilidad.

La administración de contraseñas se refiere a las prácticas de seguridad estándar de generar y mantener contraseñas de recursos e incluye aspectos como contraseñas complejas, no compartir contraseñas, cambios de contraseñas a intervalos regulares y transferencia de contraseñas de manera segura.

Una estructura de informes clara establece el proceso de autorización y rendición de cuentas porque cada empleado necesita obtener las aprobaciones del supervisor en cuestión y es responsable ante el supervisor por cumplir con los objetivos de seguridad de la organización.

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender y aplicar conceptos fundamentales de operaciones de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, monitor de privilegios especiales

Pregunta #46 de 163

Id. de pregunta: 1111770

Durante una investigación de incidente reciente, extrajo datos ocultos de la imagen de datos que se creó. ¿En qué paso del proceso de investigación de incidentes estuvo involucrado?

✗ **A)** colección
✓ **B)** examen
✗ **C)** preservación
✗ **D)** identificación

Explicación

Usted estuvo involucrado en la etapa de examen del proceso de investigación de incidentes. Este paso incluye trazabilidad, técnicas de validación, técnicas de filtrado, coincidencia de patrones, detección de datos ocultos y extracción de datos ocultos.

Usted no estuvo involucrado en el paso de identificación del proceso de investigación de incidentes. Este paso puede incluir la detección de eventos/delitos, la resolución de firmas, la detección de perfiles, la detección de anomalías, la recepción de quejas, la supervisión del sistema y el análisis de auditoría.

Usted no estuvo involucrado en el paso de preservación del proceso de investigación de incidentes. Este paso puede incluir tecnologías de imágenes, estándares de cadena de custodia y sincronización de tiempo.

No participó en el paso de recopilación del proceso de investigación de incidentes. Este paso puede incluir métodos de recopilación aprobados, software aprobado, hardware aprobado, autoridad legal, muestreo, reducción de datos y técnicas de recuperación.

Los pasos apropiados en una investigación forense son los siguientes:

- Identificación
- Preservación
- Colección
- Examen
- Análisis
- Presentación
- Decisión

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender y apoyar las investigaciones

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 7: Operaciones de Seguridad, Investigaciones Forenses y Digitales

---

Pregunta #47 de 163

Id. de pregunta: 1105503

¿Quién es responsable de aprobar las solicitudes de cambio?

- ✓ **A)** tablero de control de cambios
- ✗ **B)** propietario del activo
- ✗ **C)** administrador de cambios
- ✗ **D)** cambiar de propietario

Explicación

La junta de control de cambios (CCB) es responsable de aprobar las solicitudes de modificación.

El propietario del cambio suele ser la persona que solicita el cambio, pero otra persona, como el propietario del activo, también puede solicitar el cambio. El administrador de cambios administra el proceso general de administración de cambios, pero no es el único responsable de aprobar las solicitudes de cambio.

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender y participar en los procesos de gestión del cambio

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 7: Operaciones de seguridad, procesos de gestión de cambios

---

Pregunta #48 de 163

Id. de pregunta: 1111766

Su organización ha sido víctima recientemente de un ataque de red. ¿Quién realiza los procedimientos de emergencia en respuesta a este ataque?

- ✓ **A)** el equipo de respuesta a incidentes

- ✗ **B)** el equipo de seguridad cibernética
- ✗ **C)** el equipo de detección de intrusiones
- ✗ **D)** el equipo de prevención de incidentes

Explicación

Los procedimientos de emergencia en respuesta a un sistema informático o ataque de red son realizados por el equipo de respuesta a incidentes. Los incidentes de seguridad que se producen dentro de la organización son manejados por el equipo de respuesta a incidentes. El equipo está formado por miembros de diferentes departamentos de la organización, como los representantes de la alta dirección, el departamento de tecnología de la información, el departamento jurídico y el departamento de recursos humanos.

El equipo central de respuesta a incidentes debe tener conocimientos técnicos sólidos y debe seguir procedimientos estándar y formales para el manejo de incidentes. El propósito principal del manejo de incidentes informáticos es contener y reparar cualquier daño causado por un evento. Después de responder a un incidente, se debe celebrar una reunión dentro de una semana para discutir la intrusión y su investigación. El análisis debería resultar útil para prevenir futuros ataques y mejorar los procedimientos de respuesta de emergencia.

Los siguientes puntos están en la agenda del equipo de respuesta a incidentes mientras se investiga un incidente:

- Puntos de contacto e informes fuera de la empresa
- Puntos de contacto para la ciencia forense del sistema
- Proceso utilizado para buscar y asegurar la evidencia, incluidos los miembros del equipo de búsqueda e incautación
- Contenido y formato del informe que se presentará a la administración
- Métodos para tratar con diferentes tipos de sistemas

El equipo de respuesta a incidentes también debe preocuparse por el hecho de que un sospechoso puede intentar destruir pruebas.

Los equipos de prevención de incidentes, detección de intrusiones y seguridad cibernética no se ocupan de la respuesta a incidentes.

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender y apoyar las investigaciones

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, gestión de incidentes

---

Pregunta #49 de 163

Id. de pregunta: 1192973

¿Cuál de los siguientes ejercicios de continuidad de las actividades puede ser bastante complicado y debe realizarse anualmente?

✗ **A)** ejercicio de sobremesa

✓ **B)** pruebas de simulación de desastres

✗ **C)** simulacro de evacuación de emergencia

✗ **D)** tutorial estructurado

Explicación

Las pruebas de simulación de desastres pueden ser bastante involucradas y deben realizarse anualmente. Para completar esta prueba, debe crear una simulación de un desastre real, incluidos todos los equipos, suministros y personal necesarios. Esta prueba determinará si puede llevar a cabo funciones empresariales críticas durante el evento.

Ninguno de los otros ejercicios es tan complicado como las pruebas de simulación de desastres.

En un ejercicio de mesa, el personal de cada unidad de negocio que entiende la recuperación ante desastres se reúne en una sala de conferencias para examinar el plan y buscar lagunas.

Un tutorial estructurado se produce cuando cada miembro del equipo recorre los componentes de su plan para identificar debilidades, normalmente con un desastre específico en mente.

Los simulacros de evacuación de emergencia generalmente se completan al menos dos veces al año, y solo garantizan que el personal sepa cómo evacuar adecuadamente las instalaciones.

Objetivo:
Operaciones de seguridad

Subobsecución:
Participar en la planificación y los ejercicios de continuidad del negocio (BC)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, prueba de simulación

---

Pregunta #50 de 163

Id. de pregunta: 1192962

¿Qué principio de control de acceso garantiza que una función determinada tenga más de una persona capacitada para desempeñar sus funciones?

✗ **A)** privilegio mínimo

✗ **B)** separación de funciones

✓ **C)** rotación de trabajos

✗ **D)** denegar implícita

Explicación

La rotación de puestos de trabajo garantiza que un rol en particular tenga más de una persona capacitada para desempeñar sus funciones. El personal debe rotarse periódicamente, especialmente en puestos importantes. La rotación de puestos de trabajo y la separación de funciones también ayudan a prevenir la colusión.

Las vacaciones obligatorias son controles administrativos que aseguran que los usuarios tomen sus vacaciones para que se puedan descubrir actividades fraudulentas y se pueda llevar a cabo la rotación de trabajo.

La separación de funciones requiere la participación de más de una persona para llevar a cabo una tarea crítica. La separación de funciones garantiza que ninguna persona pueda comprometer un sistema, y se considera valiosa para disuadir el fraude. Cuando se evitan conflictos de intereses mediante la asignación de personal para completar determinadas tareas de seguridad, se está implementando la separación de funciones. Para cometer un acto ilegal, la colusión debe ocurrir entre el personal. La separación de funciones es una medida preventiva.

Las dos categorías de la política de separación de funciones son los controles dobles y la separación funcional. El control dual requiere que dos o más sujetos actúen juntos simultáneamente para autorizar una operación. La separación funcional implica un proceso de aprobación secuencial, como requerir la aprobación de un administrador para enviar una comprobación generada por un subordinado.

Además, la separación de funciones puede ser estática o dinámica. La separación estática de tareas se refiere a la asignación de individuos a roles y la asignación de transacciones a roles. En la separación estática de funciones, un individuo puede ser un iniciador de la transacción o el autorizador de la transacción. En la separación dinámica de deberes, un individuo puede iniciar y autorizar transacciones.

El principio de privilegios mínimos concede a los usuarios solo los permisos que necesitan para realizar su trabajo. Limitar el acceso de los usuarios a las cuentas administrativas forma parte de este principio. Una directiva de seguridad necesaria se basa en el principio de privilegios mínimos. El principio de privilegio mínimo se asocia más comúnmente con el control de acceso obligatorio (MAC). Al implementar este principio, los usuarios solo deben usar sus cuentas de nivel administrativo al realizar tareas de nivel administrativo. Para realizar otras tareas de nivel inferior, los mismos usuarios deben usar una cuenta de nivel inferior con los permisos mínimos que necesitan.

Una denegación implícita garantiza que determinados usuarios no pueden tener acceso a un determinado archivo, carpeta o aplicación. Una denegación implícita invalida todos los demás permisos, incluido un permiso explícito.

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender y aplicar conceptos fundamentales de operaciones de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, Rotación de trabajos

---

Pregunta #51 de 163

Id. de pregunta: 1105523

¿Qué elemento del plan de continuidad de las actividades se ocupa principalmente de minimizar los daños a la propiedad y prevenir la pérdida de vidas?

- ✗ **A)** análisis de impacto en el negocio (BIA)
- ✗ **B)** análisis del riesgo
- ✓ **C)** plan de recuperación ante desastres
- ✗ **D)** análisis de vulnerabilidades

Explicación

El plan de recuperación en casos de desastre se ocupa principalmente de reducir al mínimo los daños a la propiedad y prevenir la pérdida de vidas. La preocupación más importante durante un desastre es la seguridad del personal. El plan de recuperación ante desastres se crea para garantizar que su empresa pueda reanudar sus operaciones de manera oportuna. Como parte del plan de continuidad del negocio, el plan de recuperación ante desastres se centra en procedimientos alternativos para procesar transacciones a corto plazo. Se lleva a cabo cuando se produce la emergencia e inmediatamente después de la emergencia. La organización tiene la responsabilidad de continuar con los salarios u otros fondos para los empleados y/o familias afectadas por el desastre.

Un análisis de vulnerabilidades identifica las vulnerabilidades de su empresa. Forma parte del plan de continuidad del negocio. Su objetivo es acceder a qué áreas de su empresa están en mayor riesgo durante cualquier tipo de desastre.

Se crea un análisis de impacto empresarial (BIA) para identificar las funciones vitales y priorizarlas en función de las necesidades. Se identifican las vulnerabilidades y amenazas, y se calculan los riesgos.

Un análisis de riesgos es parte de la BIA. Se utiliza para calcular el riesgo para descubrir qué funciones ofrecerían la mayor pérdida financiera a la empresa.

Objetivo:
Operaciones de seguridad

Subobsecución:
Implementar procesos de recuperación ante desastres (DR)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y gestión de riesgos, recuperación ante desastres y el plan de recuperación ante desastres (DRP)

Pregunta #52 de 163

Id. de pregunta: 1113997

La policía local se pone en contacto con usted con respecto a un delito informático reciente. Usted proporciona evidencia a los investigadores. Los investigadores le dicen que la evidencia que usted proporcionó es evidencia corroborativa. ¿Qué afirmación es cierta de este tipo de evidencia?

- ✓ **A)** Le permite probar un punto o una idea.
- ✗ **B)** Siempre actúa como evidencia concreta.
- ✗ **C)** A veces se puede usar solo.
- ✗ **D)** Debe ser controlado por múltiples fuentes.

Explicación

La evidencia corroborativa le permite probar un punto o una idea. La evidencia corroborativa es evidencia adicional que es creíble y admisible en el tribunal de justicia. Aunque la evidencia corroborativa no puede probar un hecho por sí sola, se utiliza para complementar otras evidencias. La evidencia corroborativa confirma, apoya o fortalece otras evidencias al hacer que la evidencia sea más probable.

Las pruebas corroborativas son mantenidas y controladas por una sola fuente independiente diferente del acusador o del acusado. Las pruebas corroborativas pueden ser de naturaleza circunstancial o directa. Deben reunirse pruebas corroborativas de fuentes independientes para confirmar que el delito se ha cometido y que el acusado lo cometió.

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender los requisitos para los tipos de investigación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, evidencia corroborativa

---

Pregunta #53 de 163

Id. de pregunta: 1113995

La red de su organización fue atacada recientemente. Durante el ataque, los hackers robaron información valiosa y patentada. Se le ha pedido que proporcione información que sea admisible como prueba en un tribunal de justicia para procesar a los sospechosos. ¿Qué debe proporcionar?

✗ **A)** copias de datos de disco duro

✓ **B)** volcados de memoria

✗ **C)** Contraseñas

✗ **D)** nombres de inicio de sesión de usuario

Explicación

Los volcados de memoria son admisibles en el tribunal de justicia como prueba para procesar a un sospechoso. Los volcados de memoria contienen el estado más reciente del sistema antes de que se produjera el ataque. Para garantizar una cadena de custodia clara para la recopilación de pruebas, el sistema debe eliminarse de la red y el contenido de la memoria debe volcarse debido a la naturaleza sensible y frágil de la información. Este volcado de memoria puede contener información vital sobre el incidente y puede resultar útil para procesar al sospechoso.

Los nombres de inicio de sesión de usuario, las contraseñas y las copias de datos del disco duro no son útiles para procesar a un sospechoso. Por lo tanto, ninguna de ellas se considera prueba admisible en el tribunal de justicia. Es posible que la policía necesite obtener contraseñas como parte de una investigación. Las fuerzas del orden pueden utilizar los siguientes métodos para obtener contraseñas:

- Utilice el software de descifrador de contraseñas.
- Obligar al sospechoso a proporcionar la contraseña.
- Póngase en contacto con el desarrollador del software para obtener información para obtener acceso a la computadora o la red a través de una puerta trasera.

Si bien las copias de datos del disco duro no son admisibles en el tribunal, el disco duro original es admisible, siempre que se mantenga la cadena de custodia adecuada y se aseguren las pruebas.

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender y apoyar las investigaciones

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, preservar y recopilar evidencia

---

Pregunta #54 de 163

Id. de pregunta: 1105456

Un usuario hereda un permiso basado en su pertenencia a grupos. ¿Qué tipo de derecho se ha aplicado?

- ✗ **A)** derecho explícito
- ✗ **B)** derecho de acceso
- ✗ **C)** capacidad
- ✓ **D)** derecho implícito

Explicación

Un derecho implícito se produce cuando un usuario hereda un permiso basado en la pertenencia a grupos. También puede producirse debido a la asignación de roles.

Una capacidad es un derecho de acceso que se asigna directamente a un sujeto.

Un derecho explícito se produce cuando a un usuario se le concede un permiso directamente.

Un derecho de acceso es un término genérico que hace referencia a cualquier permiso concedido a un usuario, ya sea implícita o explícitamente.

Objetivo:
Operaciones de seguridad

Subobsecución:
aprovisionamiento seguro de recursos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, administración de cuentas, grupos y roles

---

Pregunta #55 de 163

Id. de pregunta: 1111782

¿Cuál es el primer paso del ciclo de vida del equipo?

- ✓ **A)** Evaluación
- ✗ **B)** Adquisición e implementación
- ✗ **C)** Administración
- ✗ **D)** Jubilación

Explicación

La evaluación es el primer paso del ciclo de vida del equipo. Los pasos del ciclo de vida del equipo son los siguientes:

- Evaluación
- Adquisición e implementación
- Administración
- Jubilación

Objetivo:
Operaciones de seguridad

Subobsecución:
aprovisionamiento seguro de recursos

Referencias:

Gestión de activos de ciclo devida, https://www.lce.com/Life-Cycle-Asset-Management-1112.html

---

Pregunta #56 de 163

Id. de pregunta: 1105425

Usted es el investigador de incidentes de su organización. Debe crear dos imágenes del disco duro de un servidor de archivos. Los procedimientos de investigación de incidentes indican que debe asegurarse de que los nuevos medios se purgan correctamente.

¿Qué debe hacer para cumplir con este requisito?

✗ **A)** Asegúrese de que el nuevo medio tiene el formato correcto.
✓ **B)** Asegúrese de que el nuevo medio no contiene ningún dato residual.
✗ **C)** Asegúrese de que el nuevo medio esté correctamente etiquetado.
✗ **D)** Asegúrese de que se crean resúmenes de mensaje de los datos copiados.

Explicación

Debe asegurarse de que el nuevo medio no contenga datos residuales. Sólo los datos que se recopilan como prueba durante la investigación del incidente deben colocarse en los nuevos medios de comunicación. Se deben hacer dos copias de los medios originales. La primera copia debe almacenarse en una biblioteca para conservar el estado original de los datos. La segunda copia debe utilizarse para el análisis.

Ninguna de las otras opciones explica lo que se entiende por purgado.

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender los requisitos para los tipos de investigación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, preservar y recopilar evidencia

---

Pregunta #57 de 163

Id. de pregunta: 1105508

¿Qué solución tolerante a fallos es la más costosa de implementar?

- ✓ **A)** Racimos
- ✗ **B)** INCURSIÓN
- ✗ **C)** Backups
- ✗ **D)** controladores de disco redundantes

Explicación

Un clúster es la solución tolerante a errores más costosa de implementar de las soluciones dadas. Un clúster proporciona una solución de servidor tolerante a errores que permite que varios servidores aparezcan como un único servidor para los usuarios. Si se produce un error en uno de los servidores del clúster, los servidores restantes asumen la carga.

La matriz redundante de discos independientes (RAID) es una solución de disco tolerante a errores en la que se implementan varios discos dentro de un equipo. En general, los discos duros no son tan caros como los ordenadores.

Las copias de seguridad son una solución tolerante a errores que garantiza que los datos estén protegidos mediante copias de seguridad en cinta, disco compacto (CD) y otros medios. Por lo general, las copias de seguridad se consideran una solución económica de tolerancia a errores.

Los controladores de disco redundantes garantizan que los datos tienen varias rutas a través de las cuales conectarse a las unidades de disco duro. Los controladores de disco suelen ser menos costosos que los equipos.

Objetivo:
Operaciones de seguridad

Subobsecución:
Implementar estrategias de recuperación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 2: Seguridad de activos, tecnologías tolerantes a fallos

Pregunta #58 de 163

Id. de pregunta: 1192965

¿Cuáles de los siguientes deben ser miembros del Equipo de respuesta a incidentes de seguridad informática (CSIRT)?

a. Miembro del departamento de TI

B. Miembro del departamento legal

c. Miembro del departamento de relaciones públicas

d. Miembro del equipo directivo

- ✗ **A)** opción b
- ✗ **B)** Opción d
- ✗ **C)** opciones A y B
- ✗ **D)** opción A
- ✗ **E)** opción c
- ✓ **F)** todas las opciones
- ✗ **G)** Opciones C y D

Explicación

El equipo de respuesta a incidentes de seguridad informática (CSIRT) debe contener los siguientes miembros:

- Líder de equipo de CSIRT
- CSIRT Incidente Líder
- Miembros Asociados de CSIRT, incluyendo
  - Miembro del departamento de TI
  - Miembro del departamento legal o asesor legal
  - Miembro del equipo de relaciones públicas
  - Miembro del equipo directivo

Los miembros del equipo tienen roles específicos durante una investigación de incidentes. El CSIRT tiene las siguientes responsabilidades durante una investigación de incidente:

- Evaluación inicial - propiedad de CSIRT Incident Lead
- Respuesta inicial - propiedad de CSIRT Incident Lead
- Colección de evidencia forense - propiedad de un miembro del departamento legal
- Implementación de arreglos temporales: propiedad de CSIRT Incident Lead
- Comunicación de incidentes - propiedad de un miembro del equipo de administración

- Contacto local de aplicación de la ley - propiedad de un miembro del equipo de administración
- Implementación de arreglos permanentes : propiedad de CSIRT Incident Lead
- Determinación del impacto financiero - propiedad del miembro del equipo de gestión

Como parte de una investigación de incidentes, la organización debe tener reglas de compromiso establecidas que definan todos los roles y responsabilidades de un incidente de seguridad. Estas normas deben revisarse y actualizarse periódicamente para asegurarse de que están actualizadas. Las reglas de compromiso definen cómo el CSIRT debe manejar el incidente y qué acciones son legales. El asesoramiento jurídico y las fuerzas del orden locales deberían participar en la elaboración de las normas para entablar combate. Además, las normas para entablar combate deben conceder autorización a los miembros del equipo del CSIRT para desempeñar sus funciones. El alcance de los deberes de los miembros del equipo de CSIRT debe estar claramente definido para evitar cualquier problema legal futuro.

Objetivo:
Operaciones de seguridad

Subobsecución: Llevar
a cabo la gestión de incidentes

Referencias:

En respuesta a incidentes de seguridad de TI, HYPERLINK "https://technet.microsoft.com/en-us/library/cc700825.aspx" \t "sean" http://technet.microsoft.com/en-us/library/cc700825.aspx

---

Pregunta #59 de 163

Id. de pregunta: 1114775

¿Qué afirmaciones con respecto a una pista de auditoría NO son ciertas?

un. Una pista de auditoría es un control preventivo.

B. Una pista de auditoría ayuda en la detección de intrusiones.

c. Una pista de auditoría no registra los intentos de inicio de sesión correctos.

d. Una pista de auditoría establece la responsabilidad por el control de acceso.

E. Una pista de auditoría no se revisa tan pronto como se detecta una intrusión.

✗ **A)** opciones b, d y e

✗ **B)** opción e

✓ **C)** opciones a, c y e

✗ **D)** opción A

- ✗ **E)** opción b
- ✗ **F)** Opción d
- ✗ **G)** opción c

Explicación

Una pista de auditoría no es un control preventivo. Es un control detectivesco que mantiene un registro secuencial de las actividades del sistema y el uso de recursos del sistema.

Una pista de auditoría registra una gran cantidad de información útil, como intentos de inicio de sesión correctos y no exitosos, identificación del usuario, uso de contraseña y recursos a los que accede un usuario durante un período de tiempo. Las pistas de auditoría también pueden proporcionar información sobre eventos relacionados con el sistema operativo y la aplicación.

Los registros de seguimiento de auditoría normalmente se revisan antes de que se haya detectado y contenido una intrusión. Antes de que se vuelva a instalar el sistema afectado y se reinicie la producción, los registros de seguimiento de auditoría le permiten realizar un seguimiento del origen de la intrusión, comprender el tipo de ataque e identificar una laguna que puede dar lugar a una posible infracción de seguridad en el futuro.

El propósito principal de los registros y pistas de auditoría es establecer la responsabilidad individual.

El acceso a los registros y seguimientos de auditoría debe controlarse estrictamente. Además, los datos registrados en un registro de auditoría deben controlarse estrictamente. La separación de funciones debe hacerse cumplir para garantizar que el personal que administra la función de control de acceso y el personal que administra la pista de auditoría sean dos personas diferentes.

Un administrador de seguridad debe revisar periódicamente las pistas de auditoría para detectar cualquier actividad sospechosa o un cuello de botella de rendimiento en los recursos de infraestructura. Un administrador puede seleccionar ciertos eventos críticos y registrarlos para su revisión. Posteriormente, el administrador puede utilizar los eventos para el análisis.

En lugar de revisar manualmente una gran cantidad de datos de pistas de auditoría, se pueden utilizar aplicaciones y herramientas de análisis de pistas de auditoría para reducir el volumen de registros de auditoría y mejorar la eficiencia del proceso de revisión. Estas herramientas de análisis se pueden utilizar para proporcionar información sobre eventos específicos en un formato útil y con suficientes detalles.

Objetivo:
Operaciones de seguridad

Subobsecución:
Llevar a cabo actividades de registro y vigilancia

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, Detective

Pregunta #60 de 163

Id. de pregunta: 1105476

Como miembro del equipo de seguridad de su organización, está examinando todos los aspectos de la seguridad de las operaciones de la red. Debe determinar las contramedidas que se pueden utilizar en la seguridad de las operaciones. Ya ha examinado los recursos y la información que deben protegerse. ¿Cuál es el tercer tipo de activo que debe examinarse?

✗ **A)** personal

✗ **B)** servidores de red

✗ **C)** medios de red

✓ **D)** hardware

Explicación

También debe examinar el hardware en el que residen los recursos y la información. La seguridad de las operaciones examina las contramedidas utilizadas para proteger los recursos, la información y el hardware en el que residen los recursos y la información.

Ninguna de las otras opciones es correcta.

El personal no son activos que deba examinarse en la seguridad de las operaciones. La seguridad de las operaciones se ocupa de proteger los recursos, la información y el hardware en el que residen los recursos y la información. La administración es responsable del personal.

Los medios de red y los servidores de red pueden formar parte del hardware que se examina durante la seguridad de las operaciones. Sin embargo, cualquiera de esas opciones no es el único tipo de activo que debe examinarse.

Objetivo:
Operaciones de seguridad

Subobjecución:
Aplicar técnicas de protección de recursos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, activos de información

Pregunta #61 de 163

Id. de pregunta: 1192974

Su organización tiene una caja fuerte para almacenar equipos portátiles corporativos cuando no se están utilizando. Como parte del plan de seguridad, debe asegurarse de que la caja fuerte enganche un bloqueo adicional si la temperatura de la caja fuerte excede un cierto nivel. Esto proporcionará protección contra la perforación. ¿Qué tipo de bloqueo debe implementar?

- ✗ **A)** rebloqueo activo
- ✓ **B)** relock térmico
- ✗ **C)** relock pasivo
- ✗ **D)** bloqueo de ranura

Explicación

Debe implementar un relock térmico. Los relocks térmicos activan un bloqueo adicional cuando se cumple una cierta temperatura. Esta es una buena función para proporcionar para evitar que los ladrones de perforar la caja fuerte.

Un relock pasivo detecta cuando alguien intenta manipularlo. Cuando se produce esta detección, los pernos internos adicionales caerán en su lugar para evitar el compromiso.

Un bloqueo de ranura es un bloqueo utilizado para conectar un portátil a un objeto estacionario.

Un bloqueo activo no es un tipo válido de bloqueo seguro.

Objetivo:
Operaciones de seguridad

Subobjetiva:
Implementar y administrar la seguridad física

Referencias:

Dispositivos de rebloqueo, HYPERLINK "http://www.tomziemer.com/2014/08/relock-devices-types.html" \t "sean" http://www.tomziemer.com/2014/08/relock-devices-types.html

---

Pregunta #62 de 163

Id. de pregunta: 1105524

Un terremoto dañó el edificio que alberga el centro de datos de su organización. Como resultado, el sitio alternativo en Nueva Jersey debe configurarse y ponerse en línea. ¿Qué equipo debería ser responsable de esto?

- ✗ **A)** equipo de evaluación de daños
- ✓ **B)** equipo de restauración
- ✗ **C)** equipo de salvamento

✗ **D)** equipo de seguridad

Explicación

El equipo de restauración debe ser responsable de configurar el sitio alternativo y ponerlo en línea cuando se produce un desastre. Al configurar este sitio alternativo, las funciones empresariales más críticas deben ponerse en línea primero. Para que esto ocurra, los niveles de prioridad de las funciones empresariales deben definirse en el plan de recuperación ante desastres. Sin estos niveles de prioridad, es posible que el negocio no esté operativo dentro del plazo de recuperación.

El equipo de salvamento es responsable de la recuperación del sitio original. Esto se denomina fase de reconstitución. En el plan de recuperación en casos de desastre debería explicarse cómo debería aplicarse la fase de reconstitución. Las funciones menos críticas deben moverse primero al sitio original para garantizar que las funciones empresariales críticas no se vean afectadas negativamente debido a errores de conectividad o instalación.

El equipo de seguridad es responsable de evaluar la seguridad en el sitio alternativo y primario cuando se produce un desastre.

El equipo de evaluación de daños es responsable de evaluar los daños en el sitio primario cuando ocurre un desastre. Esto incluye estimar cuánto tiempo se tardará en poner en línea las funciones críticas.

Todos estos equipos apoyan el plan de recuperación ante desastres, que tiene como objetivo minimizar los riesgos asociados con un desastre.

Objetivo:
Operaciones de seguridad

Subobsecución:
Implementar procesos de recuperación ante desastres (DR)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, equipo de restauración

---

Pregunta #63 de 163

Id. de pregunta: 1105438

Su empresa supervisa varios eventos para asegurarse de que la seguridad de los servidores no se ve comprometida y que el rendimiento de los servidores se mantiene dentro de ciertos umbrales.

Un consultor de seguridad ha sido contratado por su empresa para analizar las medidas de seguridad de la organización. El consultor ha solicitado acceso a los registros de supervisión de seguridad. Debe limitar la cantidad de información del registro de auditoría que proporciona descartando la información que no necesita el consultor. ¿Qué herramienta debe utilizar?

✗ **A)** herramienta de detección de varianza

✗ **B)** filtro de auditoría

✗ **C)** herramienta de detección de firmas de ataques

✓ **D)** herramienta de reducción de auditoría

Explicación

Debe utilizar una herramienta de reducción de auditoría. Una herramienta de reducción de auditoría se utiliza para limitar la cantidad de información del registro de auditoría descartando la información que no necesita el profesional de la seguridad. Esta herramienta descarta información mundana que no es necesaria.

Un filtro de auditoría no es una herramienta. Un filtro de auditoría forma parte del registro de auditoría que permite filtrar el registro en función de determinados criterios. Debido a su función limitada, la herramienta de reducción de auditoría suele ser una mejor opción para limitar la cantidad de información que se muestra.

Una herramienta de detección de varianza supervisa las tendencias de uso para alertar a los profesionales de la seguridad de una actividad inusual.

Una herramienta de detección de firmas de ataque supervisa la red y compara los eventos con una base de datos de patrones de ataque conocidos.

Objetivo:
Operaciones de seguridad

Subobsecución:
Llevar a cabo actividades de registro y vigilancia

Referencias:

Herramientas de reducción de auditorías, https://definedterm.com/audit_reduction_tools

---

Pregunta #64 de 163

Id. de pregunta: 1105457

¿Qué es un término que es sinónimo de etiqueta de seguridad?

✗ **A)** tabla de capacidades

✗ **B)** lista de control de acceso (ACL)

✓ **C)** etiqueta de confidencialidad

✗ **D)** regla

Explicación

Etiqueta de confidencialidad es un término que es sinónimo de etiqueta de seguridad. Las etiquetas de seguridad se utilizan en un entorno de control de acceso obligatorio (MAC) para determinar el nivel de seguridad de los sujetos y objetos.

Una regla se utiliza en un entorno de control de acceso basado en reglas y no es lo mismo que una etiqueta de seguridad.

Una tabla de capacidades forma parte de la matriz de control de acceso. Muestra los permisos concedidos a un sujeto en objetos. No es lo mismo que una etiqueta de seguridad.

Una lista de control de acceso (ACL) forma parte de la matriz de control de acceso. Muestra el permiso concedido a un objeto y los sujetos a los que se han concedido esos permisos. No es lo mismo que una etiqueta de seguridad.

Objetivo:
Operaciones de seguridad

Subobsecución:
aprovisionamiento seguro de recursos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Control de acceso obligatorio de gestión de identidad y acceso

---

Pregunta #65 de 163

Id. de pregunta: 1192967

¿Qué afirmación es cierta para el modo de seguridad dedicado?

- ✗ **A)** Algunos usuarios tienen la autorización y la aprobación formal necesarias para acceder a todos los datos.
- ✗ **B)** Algunos usuarios tienen la autorización y la aprobación formal necesarias para acceder a algunos de los datos.
- ✓ **C)** Todos los usuarios tienen la autorización y la aprobación formal necesarias para acceder a todos los datos.
- ✗ **D)** Todos los usuarios tienen la autorización y la aprobación formal necesarias para acceder a algunos de los datos.

Explicación

Todos los usuarios en el modo de seguridad dedicado tienen la autorización y la aprobación formal requerida para acceder a todos los datos procesados por el sistema.

El sistema de modo de seguridad dedicado administra un único nivel de clasificación de la información. En un modo de seguridad dedicado, los usuarios deben firmar acuerdos de confidencialidad para acceder a los datos. El modo de seguridad dedicado proporciona un único nivel de seguridad. Por lo tanto, todos los usuarios que acceden al sistema tienen el nivel más alto de autorización de seguridad que coincide con la clasificación de los datos. Por ejemplo, los usuarios que acceden a datos que han sido clasificados como "confidenciales" deben tener la autorización de seguridad de confidencial y superior.

Otros dos conceptos esenciales son el modo de alta seguridad del sistema y el modo de seguridad multinivel. En el modo alto del sistema, el sistema de información funciona al más alto nivel de clasificación de la información. En este modo, todos los usuarios deben tener autorizaciones de seguridad para el nivel más alto de información clasificada. El modo de operación de varios niveles admite usuarios con diferentes autorizaciones y datos en múltiples niveles de clasificación.

Objetivo:
Operaciones de seguridad

Subobsecución:
Operar y mantener medidas detectivescas y preventivas

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, modo de seguridad dedicado

---

Pregunta #66 de 163

Id. de pregunta: 1192969

Su organización implementa un esquema de copia de seguridad completa/diferencial. Una copia de seguridad completa se completó hace dos días. Ayer se completó una copia de seguridad diferencial. ¿Qué archivos se respaldaron ayer?

- ✓ **A)** Todos los archivos de un conjunto de copia de seguridad que se cambiaron o crearon desde la última copia de seguridad completa
- ✗ **B)** Todos los archivos de un conjunto de copia de seguridad que se cambiaron o crearon desde la última copia de seguridad incremental
- ✗ **C)** Todos los archivos de un conjunto de copia de seguridad
- ✗ **D)** Todos los archivos de un conjunto de copia de seguridad que se cambiaron o crearon desde la última copia de seguridad diferencial

Explicación

Una copia de seguridad diferencial realiza una copia de seguridad de los archivos de un conjunto de copia de seguridad que se agregaron o cambiaron desde la última copia de seguridad completa. Un tipo de copia de seguridad diferencial crece a medida que avanza la semana y no se han realizado nuevas copias de seguridad completas. Para restaurar los datos en un esquema de copia de seguridad completa/diferencial, debe restaurar la copia de seguridad completa más reciente y la copia de seguridad diferencial más reciente que se produjo desde la última copia de seguridad completa.

Una copia de seguridad completa, a veces denominada copia de seguridad de archivo, realiza una copia de seguridad de todos los archivos de un conjunto de copia de seguridad.

Una copia de seguridad incremental realiza una copia de seguridad de todos los archivos de un conjunto de copia de seguridad que se crearon o cambiaron desde la última copia de seguridad de cualquier tipo. Para restaurar los datos en un esquema de copia de seguridad completa o incremental, debe restaurar la copia de seguridad completa más reciente y, a continuación, restaurar en orden todas las copias de seguridad incrementales que se han producido desde la copia de seguridad más reciente.

Los administradores deben considerar la posibilidad de realizar copias de seguridad periódicas de la información en los equipos de la red para protegerse contra la pérdida de datos, que puede deberse al mal uso del equipo, la infiltración de piratas informáticos o el fallo del equipo.

Objetivo:
Operaciones de seguridad

Subobsecución:
Implementar estrategias de recuperación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, tipos de copia de seguridad de datos y esquemas

---

Pregunta #67 de 163

Id. de pregunta: 1105526

¿Qué instalación de copia de seguridad es propiedad de la empresa y se puede en línea con relativa facilidad?

- ✗ **A)** sitio frío
- ✓ **B)** sitio redundante
- ✗ **C)** sitio cálido
- ✗ **D)** sitio caliente

Explicación

Un sitio redundante es una instalación de copia de seguridad que es propiedad de la empresa y se puede llevar a la línea con relativa facilidad. También es gestionado por la empresa. En la mayoría de los casos, un sitio redundante está caliente, lo que significa que está listo para la producción inmediatamente. Si se produce un desastre en el sitio primario, el sitio redundante se pone en línea con relativa facilidad.

Un sitio caliente es una instalación de copia de seguridad que es propiedad de otra empresa y se puede llevar a la línea con relativa facilidad. La empresa que necesita los servicios de copia de seguridad paga una tarifa al propietario. El propietario es responsable de la gestión del sitio caliente. Si se produce un desastre en el sitio primario, el sitio caliente se pone en línea rápida y fácilmente.

Un sitio caliente es una instalación de copia de seguridad que es propiedad de otra empresa y está parcialmente configurada, normalmente excluyendo los servidores. Si se produce un desastre en el sitio primario, la empresa que necesita el servicio llevaría el hardware y el software al sitio en caliente para la instalación. La mejor manera de garantizar que las cintas de backup de la empresa se puedan restaurar y utilizar en un sitio cálido es recuperar las cintas de la instalación fuera del sitio y verificar que el equipo en el sitio original pueda leer los datos.

Un sitio frío es una instalación de respaldo que es propiedad de otra compañía y solo incluye un alquiler de habitación básico, como electricidad, aire acondicionado, plomería, etc. Si se produce un desastre en el sitio primario, el sitio frío tendría que configurarse por completo, a veces tardando semanas en configurarse.

Todas estas entidades a veces se conocen como reemplazos de almacenamiento fuera del sitio. Las instalaciones fuera del sitio deben estar lo suficientemente lejos de la instalación original para que el mismo desastre no afecte a ambos lugares.

Nota: En el contexto del examen CISSP, los sitios calientes se refieren siempre a los sitios poseídos por otra parte. Los sitios redundantes siempre hacen referencia a sitios propiedad de la empresa que necesita el servicio. Los sitios redundantes pueden ser sitios calientes, cálidos o fríos.

Objetivo:
Operaciones de seguridad

Subobsecución:
Implementar procesos de recuperación ante desastres (DR)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, recuperación y estrategias de múltiples sitios

---

Pregunta #68 de 163

Pregunta con id.: 1114000

Como parte del mantenimiento de rutina, su organización requiere que los administradores del sistema realicen una revisión y auditoría de acceso de rutina. Como parte de este proceso, decide auditar el acceso de los usuarios a

archivos y carpetas. ¿Qué directiva de auditoría de Windows debe habilitar?

- ✗ **A)** Acceso al servicio de directorio
- ✗ **B)** Eventos de inicio de sesión de cuenta
- ✗ **C)** Eventos de inicio de sesión
- ✓ **D)** Acceso a objetos

Explicación

Debe habilitar la auditoría de acceso a objetos. Esta directiva de auditoría audita el acceso a archivos, carpetas, impresoras y otros objetos.

Si audita los eventos de inicio de sesión, audita cuando alguien ha iniciado o apagado un equipo. Si audita los eventos de inicio de sesión de cuenta, audita cuando alguien ha iniciado sesión en un controlador de dominio. Si audita el acceso al servicio de directorio, se audita cuando alguien tiene acceso a un objeto de Active Directory.

Objetivo:
Operaciones de seguridad

Subobsecución:
Llevar a cabo actividades de registro y vigilancia

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, tipos de auditoría

---

Pregunta #69 de 163

Id. de pregunta: 1105415

Usted está realizando una investigación forense de una reciente violación de la seguridad informática. Se le ha pedido que utilice imágenes de disco para crear una copia del contenido de un disco duro. ¿Qué afirmación es cierta de las imágenes de disco cuando se realiza en una investigación forense?

- ✗ **A)** Una copia a nivel de bytes del disco ayuda en la investigación forense.
- ✓ **B)** Una copia a nivel de bits del disco ayuda en la investigación forense.
- ✗ **C)** No se debe volcar el contenido de la memoria.
- ✗ **D)** Se debe utilizar la copia original del disco.

Explicación

Una copia a nivel de bits del disco original resulta útil en la investigación forense. Una copia a nivel de bits de un disco duro se refiere a hacer una copia a nivel de sector para cubrir cada parte del área que puede almacenar datos de usuario, como espacio de holgura y espacio libre.

No se prefiere una copia a nivel de bytes del disco duro para el análisis forense después de que se haya producido un incidente. Una copia a nivel de bytes inicia la creación de imágenes forenses de la estación de trabajo atacada.

Para garantizar la integridad de las pruebas, la investigación forense no se realiza en el sistema real. El sistema se desconecta desconectándolo de la red, descargando el contenido de la memoria y apagándolo. Se toma una copia de seguridad del sistema y esta copia de seguridad se utiliza con fines de investigación. La salida del software de imágenes forenses debe dirigirse hacia una unidad de interfaz de sistema de equipo (SCSI) pequeña o algún otro medio que sea externo al sistema que se está investigando. Esto se hace para iniciar la proyección de imagen forense de la estación de trabajo atacada.

Cambiar los elementos del sistema, como cambiar las marcas de tiempo de los archivos y modificarlos, puede destruir la evidencia. Por lo tanto, el personal calificado debe realizar la investigación forense para garantizar que las pruebas no están ilesas ni corrompas.

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender los requisitos para los tipos de investigación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, análisis de medios

---

Pregunta #70 de 163

Id. de pregunta: 1105549

Su centro de datos tiene su propio bloqueo para evitar la entrada. El plan de seguridad de su organización indica que el bloqueo del centro de datos debe ser programable. ¿Qué tipo de bloqueo debe utilizar?

- ✗ **A)** bloqueo mecánico
- ✗ **B)** cerradura del vaso
- ✗ **C)** cerradura de combinación
- ✓ **D)** bloqueo de cifrado

Explicación

Un bloqueo de cifrado es un bloqueo que es programable. Los bloqueos de cifrado no tienen llave. Los usuarios deben introducir el cifrado adecuado utilizando el teclado del candado.

Ninguna de las otras opciones es correcta.

Los dos tipos principales de cerraduras mecánicas son cerraduras de la salada y cerraduras del vaso.

Las cerraduras con warded son candados básicos. La cerradura tiene salas (proyecciones de metal alrededor del ojo de la cerradura), y sólo una llave en particular trabajará con las salas para desbloquear la cerradura.

Una cerradura de vaso tiene más piezas que una cerradura de caja. La llave cabe en el cilindro, elevando las piezas de la cerradura a la altura correcta. Hay tres tipos de cerraduras de vaso: cerraduras de vaso de alfiler, cerraduras de vaso de oblea y cerraduras de vaso de nivel.

Los bloqueos combinados requieren la combinación correcta de números para desbloquear.

Objetivo:
Operaciones de seguridad

Subobjetiva:
Implementar y administrar la seguridad física

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Cerraduras

---

Pregunta #71 de 163

Id. de pregunta: 1105431

Su empresa ha decidido implementar la supervisión basada en anomalías en la red. Obtendrá un nuevo servidor que realizará esta supervisión. Debe asegurarse de que la supervisión es eficaz. Para que este tipo de supervisión sea eficaz, ¿qué debe existir?

- ✗ **A)** reglas
- ✗ **B)** una base de datos
- ✓ **C)** una línea de base
- ✗ **D)** respuestas activas y pasivas

Explicación

Debe existir una línea de base para que la supervisión basada en anomalías sea eficaz. La supervisión basada en anomalías detecta cualquier cambio o desviación en el tráfico de red. Con este tipo de monitoreo, hay un período de aprendizaje inicial antes de que se puedan detectar anomalías. Una vez establecidas las líneas de base, la supervisión

basada en anomalías puede detectar comportamientos anómalos. A veces, la línea de base se establece a través de un proceso manual.

Debe existir una base de datos para la supervisión basada en firmas. La supervisión basada en firmas requiere que las actualizaciones se obtengan regularmente para garantizar su eficacia. La supervisión basada en firmas vigila las intrusiones que coinciden con una identidad o firma conocida cuando se comparan con una base de datos que contiene las identidades de posibles ataques. Esta base de datos se conoce como la base de datos de firmas.

Deben existir reglas para la supervisión basada en el comportamiento. La supervisión basada en el comportamiento busca un comportamiento que no está permitido y actúa en consecuencia.

Las respuestas activas y pasivas deben estar en su lugar para la supervisión basada en red. La supervisión basada en red está conectada a la red en un lugar donde puede supervisar todo el tráfico de red. Implementa respuestas pasivas y activas. Las respuestas pasivas incluyen el registro, la notificación y el rechazo. Las respuestas activas incluyen la terminación de procesos o sesiones, cambios en la configuración de la red y engaño.

Objetivo:
Operaciones de seguridad

Subobsecución:
Llevar a cabo actividades de registro y vigilancia

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Ids de comunicación y seguridad de red

---

Pregunta #72 de 163

Id. de pregunta: 1111777

¿Qué actividad NO es una función de un sistema de detección de intrusiones (IDS)?

- ✗ **A)** detección de variación del patrón normal
- ✗ **B)** detección y respuesta a intrusiones
- ✓ **C)** verificación de sólo las amenazas dentro de la red
- ✗ **D)** detección y notificación de anomalías

Explicación

El IDS verifica los registros y caracteriza las amenazas tanto desde dentro como desde fuera de la red, no solo las que se encuentran dentro de la red. Un sistema de detección de intrusiones basado en red (NIDS) supervisa el tráfico en tiempo real para detectar cualquier intento de intrusión o amenaza maliciosa. Un NIDS supervisa no sólo la red interna, sino también cada segmento de red en el que está instalado.

El IDS de una organización realiza las siguientes funciones:

- Supervisa la red en busca de ataques
- Detecta anomalías en el tráfico de red
- Recopila y administra registros de auditoría para la red
- Detecta la variación de los patrones de tráfico normales
- Alerta al administrador en caso de ataque
- Responde a la penetración del sistema, ataques de denegación de servicio (DoS), ataques de análisis del sistema, etc.
- Protege los archivos del sistema que existen en los hosts y en el servidor
- Rastrea a los hackers individuales interpretando las técnicas del hacker de la base de datos de firmas o detectando desviaciones del comportamiento normal del tráfico

Un IDS proporciona responsabilidad y respuesta. La detección y respuesta de intrusiones incluye notificar a las partes adecuadas para asegurarse de que se toman medidas cuando se produce un evento, determinar la gravedad del evento y tomar medidas para eliminar los efectos del evento.

Objetivo:
Operaciones de seguridad

Subobsecución:
Llevar a cabo actividades de registro y vigilancia

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 4: Comunicación y Seguridad de red, IDS

Pregunta #73 de 163

Id. de pregunta: 1105465

Se le han dado varias sugerencias para aplicar el principio de privilegios mínimos. ¿Cuál es la mejor implementación de este principio?

✗ **A)** Asegúrese de que todos los servicios utilizan la cuenta administrativa principal para ejecutar sus procesos.

✓ **B)** Emita el mandato Ejecutar como para ejecutar tareas administrativas durante una sesión de usuario normal.

✗ **C)** Completar tareas administrativas en un equipo que funciona sólo como un servidor.

✗ **D)** Emitir una sola cuenta a cada usuario, independientemente de su función de trabajo.

Explicación

La mejor implementación del principio de privilegios mínimos es emitir el comando Ejecutar como para ejecutar tareas administrativas durante una sesión de usuario normal.

Nunca debe utilizar una cuenta administrativa para realizar operaciones rutinarias, como crear un documento, comprobar el correo electrónico, etc. Las cuentas administrativas solo se deben usar cuando necesite realizar una tarea administrativa, como configurar servicios, realizar copias de seguridad del equipo, etc. Al emitir el comando Ejecutar como para ejecutar tareas administrativas durante una sesión de usuario normal, se ejecuta la tarea según sea necesario, pero se limita solo la tarea concreta a ejecutarse bajo la cuenta administrativa. Si ha iniciado la sesión y vuelve a usar la cuenta administrativa, existe la posibilidad de que olvide volver a usar su cuenta de usuario normal al realizar tareas rutinarias.

Completar tareas administrativas en un equipo que funciona sólo como un servidor no es una implementación del principio de privilegios mínimos. Los usuarios deben poder realizar tareas administrativas en servidores y estaciones de trabajo.

Asegurarse de que todos los servicios utilizan la cuenta administrativa principal para ejecutar sus procesos es un ejemplo de NO garantizar el principio de privilegios mínimos. Los servicios deben usar una cuenta de servicio creada específicamente para el servicio que solo esté configurada con esos derechos, permisos y privilegios para que el servicio lleve a cabo sus funciones.

Emitir una sola cuenta a cada usuario, independientemente de sus funciones de trabajo, es un ejemplo de NO garantizar el principio de privilegios mínimos. A los usuarios encargados de tareas administrativas se les debe emitir un mínimo de dos cuentas: una cuenta de usuario normal para realizar tareas de usuario normales y una cuenta de usuario administrativo configurada con esos derechos, permisos y privilegios para que el usuario lleve a cabo sus tareas administrativas.

Una implementación adecuada del principio de privilegios mínimos garantiza que los usuarios solo tengan los derechos de usuario que necesitan para ejecutar sus tareas autorizadas. Los usuarios solo deben tener derechos, permisos y privilegios adecuados para realizar sus trabajos. El concepto de privilegio mínimo existe dentro de los Criterios de evaluación del sistema informático de confianza (TCSEC), que se utiliza para categorizar y evaluar la seguridad en todo el software informático.

El principio de privilegios mínimos se implementa normalmente limitando el número de cuentas administrativas. Las herramientas que es probable que sean utilizadas por los piratas informáticos deben tener permisos que sean lo más restrictivos posible.

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender y aplicar conceptos fundamentales de operaciones de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, necesidad de saber / privilegios mínimos

---

Pregunta #74 de 163

Id. de pregunta: 1111795

Al desarrollar el plan de continuidad del negocio, su equipo debe crear un plan que garantice que el funcionamiento normal se pueda reanudar de manera oportuna. ¿Qué elemento está creando tu equipo?

✗ **A)** análisis de vulnerabilidades

✗ **B)** plan de continuidad del negocio

✗ **C)** análisis de impacto en el negocio (BIA)

✓ **D)** plan de recuperación ante desastres

Explicación

El plan de recuperación ante desastres se crea para garantizar que su empresa pueda reanudar sus operaciones de manera oportuna. Como parte del plan de continuidad de las actividades, se centra principalmente en procedimientos alternativos para procesar las transacciones a corto plazo. Se lleva a cabo cuando se produce la emergencia e inmediatamente después de la emergencia.

Un análisis de vulnerabilidades identifica las vulnerabilidades de su empresa. Forma parte del plan de continuidad del negocio.

Se crea un plan de continuidad del negocio para garantizar que existan políticas para hacer frente a las interrupciones a largo plazo y los desastres para mantener las operaciones. Su objetivo principal es garantizar que la empresa mantenga sus objetivos comerciales a largo plazo tanto durante como después de la interrupción y se centra principalmente en la continuidad de la infraestructura de datos, telecomunicaciones y sistemas de información. Se deben desarrollar varios planes para cubrir todas las ubicaciones de la compañía. El plan de continuidad del negocio tiene un enfoque más amplio que el plan de recuperación ante desastres y normalmente incluye los siguientes pasos:

- Inicio de la declaración de política: incluye la redacción de la directiva para proporcionar dirección al plan de continuidad del negocio y la creación de un comité, roles y definiciones de roles del plan de continuidad del negocio.
- Creación de análisis de impacto en el negocio (BIA): incluye la identificación de vulnerabilidades, amenazas y el cálculo de riesgos. El proceso de gestión de riesgos es uno de los elementos básicos de infraestructura y servicio necesarios para dar soporte a los procesos de negocio de la organización. Esta etapa también debería identificar posibles contramedidas asociadas con cada amenaza.
- Creación de estrategias de recuperación : incluye la creación de planes para poner en línea los sistemas y las funciones rápidamente.

- Creación de planes de contingencia : incluye la redacción de directrices para garantizar que la empresa pueda operar a una capacidad reducida.
- Pruebas y capacitación : identifica las deficiencias en el plan y garantiza que el personal esté debidamente capacitado para responder adecuadamente.
- Mantenimiento del plan : garantiza que el plan se actualice regularmente.

Las pruebas del plan, el mantenimiento y la capacitación del personal incluyen una prueba formal del plan para identificar problemas que capacitan a las partes que tienen roles en el plan de continuidad del negocio para cumplir su rol y actualizan el plan según sea necesario. La empresa debe medir cuantitativamente los resultados de la prueba para asegurarse de que el plan es factible. Este paso asegura que el plan de continuidad del negocio siga siendo un foco constante de la empresa.

Los principales elementos del plan de continuidad del negocio incluyen el plan de recuperación ante desastres, la BIA, el proceso de gestión de riesgos y el plan de contingencia. Aunque debería crearse el comité del plan de continuidad de las actividades, no se considera que sea un elemento importante del plan.

Se crea un BIA para identificar las funciones vitales y priorizarlas en función de la necesidad. Se identifican las vulnerabilidades y amenazas, y se calculan los riesgos.

Uno de los elementos más críticos en un plan de continuidad del negocio es el apoyo a la administración.

Objetivo:
Operaciones de seguridad

Subobsecución:
Implementar procesos de recuperación ante desastres (DR)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y gestión de riesgos, recuperación ante desastres y el plan de recuperación ante desastres (DRP)

Pregunta #75 de 163

Id. de pregunta: 1114783

¿Cuáles son algunas de las áreas en las que los empleados deben ser capacitados para que sigan los procedimientos cuando ocurre un desastre?

a. Procedimientos de restauración

b. Procedimientos de evacuación

c. Procedimientos de investigación

d. Procedimientos de comunicación

- ✗ **A)** Opción d
- ✗ **B)** opción b
- ✓ **C)** opciones a, b y d
- ✗ **D)** opciones a, b y c
- ✗ **E)** opciones b, c y d
- ✗ **F)** opción A
- ✗ **G)** opción c

Explicación

Los empleados deben ser entrenados en procedimientos de restauración, procedimientos de evacuación y procedimientos de comunicación. Cuando ocurre un desastre, los empleados deben saber cómo reaccionar. Otras áreas de capacitación incluyen primeros auxilios, reemplazo de equipos, apagado de equipos y transporte de equipos. La organización tiene la responsabilidad de continuar con los salarios u otros

financiamiento a los empleados y/o familias afectadas por el desastre.

Los procedimientos de investigación forman parte del proceso forense que se produce cuando se descubre una infracción de seguridad. No es parte del proceso cuando ocurre un desastre.

La sensibilización y la capacitación son controles administrativos relacionados con los procedimientos de emergencia. Otros procedimientos de emergencia que son controles administrativos incluyen simulacros, inspecciones y delegación de deberes.

Objetivo:
Operaciones de seguridad

Subobsecución:
Implementar procesos de recuperación ante desastres (DR)

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, Componentes de Personal

---

Pregunta #76 de 163

Id. de pregunta: 1111773

¿Qué afirmación es cierta de una investigación de delitos informáticos?

- ✗ **A)** La evidencia no es fácil de modificar durante la investigación.
- ✗ **B)** La evidencia no es importante desde una perspectiva legal.

✓ **C)** El equipo de respuesta a incidentes de la compañía a veces no está dispuesto a involucrar a las autoridades policiales.

✗ **D)** El costo de la investigación a menudo resulta ser un elemento disuasorio antes de que comience la investigación.

Explicación

El equipo de respuesta a incidentes dentro de la compañía a veces no está dispuesto a involucrar a las autoridades policiales para investigar un delito informático. Si las autoridades hacen público el resultado de la investigación, la reputación de la empresa puede verse afectada, y la mala publicidad puede resultar en la pérdida de negocios y clientes. Los métodos utilizados por las autoridades federales durante la investigación pueden no ser aceptables para los investigadores de la empresa debido a los requisitos legales que no se aplican a un equipo de respuesta a incidentes y una investigación realizada por la empresa. Una vez que la aplicación de la ley se involucra, las restricciones de los investigadores son mayores de lo que son antes de que la aplicación de la ley esté involucrada.

Durante una investigación de delitos informáticos, es importante que la evidencia se recopile, almacene y controle de manera segura. La exactitud y la fiabilidad de las pruebas son fundamentales durante la investigación de un delito informático. La mayoría de las pruebas informáticas son de oídas y se pueden modificar fácilmente. Por lo tanto, debe asegurarse de que la evidencia no se modifique, altere o destruya antes de presentarse en el tribunal de justicia. Los servicios de un experto o de un especialista pueden utilizarse para demostrar la autenticidad de las pruebas en un tribunal de justicia. Cuando se ha producido un daño, debe tener especial cuidado al restaurar el sistema porque la evidencia puede ser destruida.

El costo de la investigación y el marco de tiempo requerido para completar la investigación nunca deben resultar disuasorios para una empresa antes de que comience una investigación sobre el delito informático.

Las siguientes preguntas se responden antes de que comience la investigación de un delito informático:

- ¿Quiénes estuvo involucrados y quiénes están afectados?
- ¿Cuáles son las implicaciones del ataque?
- ¿Dónde ocurrió el crimen?
- ¿Cuándo se produjo el ataque?
- ¿Cómo ocurrió y cómo pudo el intruso eludir las medidas de seguridad?

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender los requisitos para los tipos de investigación

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 7: Operaciones de Seguridad, Investigaciones Forenses y Digitales

Pregunta #77 de 163

Id. de pregunta: 1105477

¿Qué bloqueo de dispositivo impide el acceso a discos duros o puertos no utilizados en un equipo?

- ✗ **A)** control del interruptor periférico
- ✗ **B)** bloqueo de ranura
- ✗ **C)** trampa de cable
- ✗ **D)** control del interruptor
- ✓ **E)** control portuario

Explicación

Un control de puerto es un bloqueo de dispositivo que impide el acceso a discos duros o puertos no utilizados en un equipo.

Un control de interruptor es un bloqueo de dispositivo que impide el acceso a los interruptores de alimentación. Un bloqueo de ranura es un bloqueo de dispositivo que conecta un ordenador a un componente estacionario mediante un cable conectado a una ranura de expansión de repuesto. Un control de interruptor periférico es un bloqueo de dispositivo que se inserta entre el ordenador y la ranura de entrada del teclado para controlar la alimentación. Una trampa de cable es un bloqueo de dispositivo que asegura los dispositivos de entrada y salida mediante el uso de un cable para conectarlos a una unidad bloqueable.

Objetivo:
Operaciones de seguridad

Subobjecución:
Aplicar técnicas de protección de recursos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura de seguridad y bloqueos de ingeniería

---

Pregunta #78 de 163

Id. de pregunta: 1105548

¿Cuál de los siguientes NO es un tipo de bloqueo mecánico?

- ✓ **A)** warded
- ✗ **B)** nivel
- ✗ **C)** oblea

✗ **D)** anclar

Explicación

Una cerradura de esclusa es un tipo de cerradura mecánica, pero no una cerradura de vaso. Las cerraduras con warded son candados básicos. La cerradura tiene salas (proyecciones de metal alrededor del ojo de la cerradura), y sólo una llave en particular trabajará con las salas para desbloquear la cerradura.

Los dos tipos principales de cerraduras mecánicas son cerraduras de la salada y cerraduras del vaso.

Una cerradura de vaso tiene más piezas que una cerradura de caja. La llave cabe en el cilindro, elevando las piezas de la cerradura a la altura correcta. Hay tres tipos de cerraduras de vaso: cerraduras de vaso de alfiler, cerraduras de vaso de oblea y cerraduras de vaso de nivel.

Objetivo:
Operaciones de seguridad

Subobjetiva:
Implementar y administrar la seguridad física

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Cerraduras

---

Pregunta #79 de 163

Id. de pregunta: 1105429

Se le ha pedido que supervise el tráfico de la red. Al investigar los diferentes métodos de monitoreo, se preocupa por la supervisión que requiere actualizaciones periódicas para garantizar su eficacia. ¿Qué tipo de supervisión requiere que las actualizaciones se obtengan regularmente para garantizar su eficacia?

✓ **A)** basado en firmas

✗ **B)** basado en anomalías

✗ **C)** basado en el comportamiento

✗ **D)** basado en red

Explicación

La supervisión basada en firmas requiere que las actualizaciones se obtengan regularmente para garantizar la eficacia. La supervisión basada en firmas vigila las intrusiones que coinciden con una identidad o firma conocida cuando se comparan con una base de datos que contiene las identidades de posibles ataques. Esta base de datos se conoce como la base de datos de firmas. La base de datos de firmas debe actualizarse para que un IDS basado en firmas siga siendo efectivo.

La supervisión basada en red está conectada a la red en un lugar donde puede supervisar todo el tráfico de red. Implementa respuestas pasivas y activas. Respuestas pasivas que incluyen registro, notificación y rechazo. Las respuestas activas incluyen la terminación de procesos o sesiones, cambios en la configuración de la red y engaño.

La supervisión basada en anomalías detecta actividades que son inusuales. Con este tipo de monitoreo, hay un período de aprendizaje inicial antes de que se puedan detectar anomalías. Una vez establecidas las líneas de base, la supervisión basada en anomalías puede detectar actividades anómalas. A veces, la línea de base se establece a través de un proceso manual.

La supervisión basada en el comportamiento busca un comportamiento que no está permitido y actúa en consecuencia.

Objetivo:
Operaciones de seguridad

Subobsecución:
Llevar a cabo actividades de registro y vigilancia

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Ids de comunicación y seguridad de red

---

Pregunta #80 de 163

Id. de pregunta: 1111776

¿Qué elemento NO es un componente funcional de un sistema de detección de intrusiones (IDS)?

- ✗ **A)** fuente de información
- ✗ **B)** componente de base de datos
- ✗ **C)** análisis de informes de eventos
- ✗ **D)** respuesta
- ✓ **E)** detector de intrusiones estadísticas

Explicación

La detección estadística de intrusiones no es un componente de la detección de intrusiones, sino una función clave realizada por un IDS basado en anomalías. La detección estadística de intrusiones detecta desviaciones del patrón de comportamiento normal de un usuario, un host o una conexión de red.

Los componentes básicos de la detección de intrusiones son los siguientes:

- Fuente de información o sensor: para detectar eventos y enviar datos a un software de monitoreo centralizado
- Software de monitoreo centralizado: Para aceptar y analizar datos

- Análisis de informes de datos y eventos: para ofrecer contramedidas a un intento de intrusión
- Componentes de base de datos: para definir un patrón específico de un ataque
- Respuesta a un evento o una intrusión: para responder interviniendo automáticamente cuando se detecta una intrusión o notificando pasivamente los eventos al equipo de respuesta a incidentes

Ids puede ser agrupado y clasificado en función de sus fuentes de información. IDS puede analizar paquetes de segmentos de red como en el sistema de detección de intrusiones (NIDS) basado en red, desde aplicaciones de sistema operativo o desde software de aplicación como en el sistema de detección de intrusiones (HIDS) basado en host.

Objetivo:
Operaciones de seguridad

Subobsecución:
Llevar a cabo actividades de registro y vigilancia

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 4: Comunicación y Seguridad de red, IDS

Pregunta #81 de 163

Id. de pregunta: 1114003

La administración le ha pedido que implemente un honeypot. ¿Dónde debe residir este equipo?

✗ **A)** en la red pública
✓ **B)** sobre la zona de distensión (DMZ)
✗ **C)** en la red privada
✗ **D)** en la red privada virtual (VPN)

Explicación

Un honeypot debe residir en la zona desmilitarizada (DMZ) o en la subred filtrada. Un honeypot es un sistema informático que actúa como señuelo para los hackers. Se asemeja a un servidor legítimo para atraer a los usuarios no autorizados lejos de los sistemas críticos.

Un honeypot no debe residir en la red privada. Si el honeypot está en la red privada, esto indicaría que los hackers tendrían acceso a la parte más segura de su red.

Un honeypot no debe residir en la red pública. Usted debe colocar el honeypot en el DMZ para simular un sistema legítimo.

Un honeypot no debe residir en la red privada virtual (VPN). El acceso VPN se concede solo a usuarios de confianza. No es necesario atraer a estos usuarios utilizando un honeypot.

Objetivo:
Operaciones de seguridad

Subobsecución:
Operar y mantener medidas detectivescas y preventivas

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Comunicación y Seguridad de Red Honeypot

---

Pregunta #82 de 163

Id. de pregunta: 1113996

Está recopilando evidencia de un incidente de seguridad reciente en su organización. Debe copiar el medio original. ¿Cuál es el número mínimo de copias que debe hacer?

✗ **A)** 1
✓ **B)** 2
✗ **C)** 3
✗ **D)** 4

Explicación

Como mínimo, debe hacer dos copias del medio original. La primera copia es la copia del control que se almacena en una biblioteca. Esto conserva los datos. La segunda copia se utiliza para el análisis y la recopilación de pruebas.

Ninguna de las otras opciones es correcta.

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender y apoyar las investigaciones

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, análisis de medios

---

Pregunta #83 de 163

Id. de pregunta: 1105511

Debe proteger los datos de las redes informáticas de los picos de energía. ¿Qué debes usar?

✗ **A)** un aspersor

✗ **B)** una tarjeta clave

✗ **C)** un sistema de calefacción

✓ **D)** un supresor de sobretensiones

Explicación

Un supresor de sobretensiones protege los datos en las redes informáticas de picos de energía o sobretensiones. Los supresores de sobretensiones son controles preventivos.

Las computadoras operan en un rango de temperatura relativamente estrecho, que requiere el acondicionamiento climático de los sistemas de calefacción y aire acondicionado.

Una tarjeta clave es una medida de seguridad física que puede proteger un centro de datos y otros equipos informáticos de los piratas informáticos.

Un aspersor es un sistema de extinción de incendios que se requiere en la mayoría de los edificios de oficinas. Un aspersor rocía agua, lo que puede ser perjudicial para el equipo informático, por lo que las empresas deben considerar la instalación de sistemas de extinción de incendios que no sean de agua para proteger las computadoras en un centro de datos del fuego y el agua.

Objetivo:
Operaciones de seguridad

Subobsecución:
Implementar estrategias de recuperación

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Medidas Preventivas

---

Pregunta #84 de 163

Pregunta con ID: 1105500

Recibe un correo electrónico no solicitado de un proveedor de la aplicación que indica que una revisión de seguridad está disponible para la aplicación. La directiva de seguridad de su empresa establece que todas las aplicaciones deben actualizarse con revisiones de seguridad y Service Packs. ¿Qué debes hacer?

✗ **A)** Inserte el CD de instalación de la aplicación para instalar la revisión de seguridad.

✓ **B)** Vaya al sitio Web del proveedor para descargar la revisión de seguridad.

✗ **C)** Haga clic en el vínculo incrustado en el mensaje de correo electrónico para instalar la revisión de seguridad.

✗ **D)** Haga clic en el vínculo incrustado en el mensaje de correo electrónico para probar la revisión de seguridad.

Explicación

Debe ir al sitio Web del proveedor para descargar la revisión de seguridad. Esto garantiza que está obteniendo la revisión de seguridad directamente del proveedor. Si no encuentra ninguna información acerca de una nueva revisión de seguridad en el sitio Web del proveedor, es probable que sea víctima de una estafa por correo electrónico.

No debe hacer clic en el vínculo incrustado en el mensaje de correo electrónico para probar o instalar la revisión de seguridad. Un método común para que los hackers infecten sus sistemas es enviar un correo electrónico de aspecto oficial sobre el software que necesita. La única manera de asegurarse de que una revisión o service pack proviene del proveedor es ir al sitio Web del proveedor.

No debe insertar el CD de instalación de la aplicación para instalar la revisión de seguridad. Los CD de instalación originales no contendrán los últimos parches de seguridad o Service Packs.

Objetivo:
Operaciones de seguridad

Subobsecución:
Implementar y apoyar la gestión de parches y vulnerabilidades

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, gestión de parches y vulnerabilidades

---

Pregunta #85 de 163

Id. de pregunta: 1111778

Se le ha encomendado la tarea de diseñar la directiva de auditoría para su empresa en función de la directiva de seguridad de su empresa. ¿Cuál es el primer paso que debes dar?

✗ **A)** Realizar la auditoría.

✗ **B)** Informar de los resultados de la auditoría a la administración.

✓ **C)** Planee la estrategia de auditoría.

✗ **D)** Evaluar los resultados de la auditoría.

Explicación

Al diseñar una directiva de auditoría para su empresa, se deben seguir los siguientes pasos:

- Desarrollar la política de seguridad de la empresa.
- Planee la estrategia de auditoría.
- Realizar la auditoría.
- Evaluar los resultados de la auditoría.
- Informar de los resultados de la auditoría a la administración.
- Realizar seguimiento.

Para configurar la auditoría, debe habilitar la auditoría, configurar la auditoría en los objetos y, a continuación, revisar los registros de eventos.

Objetivo:
Operaciones de seguridad

Subobsecución:
Llevar a cabo actividades de registro y vigilancia

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Identity and Access Management Auditing and Reporting

---

Pregunta #86 de 163

Id. de pregunta: 1105532

Su organización está investigando instalaciones informáticas alternativas para asegurarse de que la organización puede funcionar si se destruye la instalación principal. ¿Cuál es la consideración más importante a la hora de elegir una instalación informática alternativa?

✗ **A)** recursos disponibles

✗ **B)** cantidad de tiempo necesario

✗ **C)** costar

✓ **D)** ubicación

Explicación

La ubicación de la instalación informática alternativa es la consideración más importante al elegir la instalación. Como resultado, la instalación alternativa debe estar ubicada a un mínimo de cinco millas de distancia. Algunas

recomendaciones establecen que una instalación alternativa debe estar a hasta 200 millas de distancia dependiendo de la criticidad de las operaciones para minimizar el impacto de los desastres regionales.

Ninguno de los otros factores importa si la instalación no está disponible debido a que se vio afectada por el mismo desastre.

El costo de la instalación alternativa suele ser una preocupación importante para las empresas. El costo se sopesará en función de la naturaleza crítica de los datos y la necesidad de una recuperación rápida. Tenga en cuenta que la recuperación ante desastres a menudo se considera incorrectamente un gasto discrecional por la mayoría de las empresas. Como resultado, puede ser necesario validar el costo de una instalación alternativa a la alta gerencia.

La cantidad de tiempo que se necesita la instalación es una preocupación. Algunos sitios están disponibles por períodos limitados de tiempo y no serían una buena opción durante un período de recuperación a largo plazo.

Los recursos disponibles en el sitio determinarían la cantidad de recursos que necesitaría configurar.

Objetivo:
Operaciones de seguridad

Subobsecución:
Probar planes de recuperación ante desastres (DRP)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, recuperación y estrategias de múltiples sitios

---

Pregunta #87 de 163

Id. de pregunta: 1111769

Cerca del final de una investigación de incidente reciente, el investigador de incidentes sugiere que su organización tome varias contramedidas recomendadas. ¿Qué etapa del proceso de investigación se está llevando a cabo?

✗ **A)** colección
✗ **B)** análisis
✓ **C)** presentación
✗ **D)** examen

Explicación

Se está llevando a cabo la etapa de presentación del proceso de investigación. Este paso puede incluir documentación, testimonio de expertos, aclaración, declaración de impacto de la misión, contramedidas recomendadas e interpretación estadística.

La etapa de recolección del proceso de investigación no se está llevando a cabo. Este paso puede incluir métodos de recopilación aprobados, software aprobado, hardware aprobado, autoridad legal, muestreo, reducción de datos y técnicas de recuperación.

La etapa de examen del proceso de investigación no se está llevando a cabo. Este paso puede incluir trazabilidad, técnicas de validación, técnicas de filtrado, coincidencia de patrones, detección de datos ocultos y extracción de datos ocultos.

La etapa de análisis del proceso de investigación no se está llevando a cabo. Este paso puede incluir trazabilidad, análisis estadístico, análisis de protocolos, minería de datos y determinación de plazos.

Los pasos apropiados en una investigación forense son los siguientes:

- Identificación
- Preservación
- Colección
- Examen
- Análisis
- Presentación
- Decisión

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender y apoyar las investigaciones

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 7: Operaciones de Seguridad, Investigaciones Forenses y Digitales

---

Pregunta #88 de 163

Id. de pregunta: 1111792

Está implementando software antivirus en la red de su organización. Todas las siguientes son directrices con respecto al software antivirus, EXCEPTO:

✗ **A)** Configure el software antivirus para analizar automáticamente los discos externos.

✗ **B)** Configure los análisis antivirus para que se produzcan automáticamente según una programación definida.

✓ **C)** Actualice las firmas antivirus sólo a través de un servidor local.

✗ **D)** Instale el software antivirus en todos los equipos servidor, equipos cliente, puntos de entrada de red y dispositivos móviles.

Explicación

No debe actualizar las firmas antivirus sólo a través de un servidor local. Las firmas antivirus se pueden actualizar a través del servidor del proveedor de software o de un servidor local. Tendría que determinar qué configuración será la mejor para su organización. Es importante asegurarse de que las actualizaciones se realizan automáticamente.

Algunas directrices con respecto al software antivirus son las siguientes:

- Instale el software antivirus en todos los equipos servidor, equipos cliente, puntos de entrada de red y dispositivos móviles.
- Configure los análisis antivirus para que se produzcan automáticamente en una programación definida.
- Configure el software antivirus para analizar automáticamente los discos externos.
- Configure las actualizaciones antivirus para que se produzcan automáticamente.
- Desarrollar un proceso de erradicación del virus en caso de infección.
- Analice todos los archivos de copia de seguridad en busca de virus.
- Desarrollar y actualizar periódicamente una directiva antivirus.

Objetivo:
Operaciones de seguridad

Subobsecución:
Operar y mantener medidas detectivescas y preventivas

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Software malicioso de administración de identidad y acceso

---

Pregunta #89 de 163

Id. de pregunta: 1114781

Recientemente, un empleado de su organización realizó copias ilegales de la propiedad intelectual de su organización. Esto es una violación directa de las políticas de empleo de su organización. Debe crear un equipo de respuesta a incidentes para investigar el delito.

¿Quién NO debe ser parte de un equipo de respuesta a incidentes?

a. Departamento de recursos humanos

b. un departamento de Relaciones Públicas

c. Personal directivo superior

d. Gobierno federal

e. Departamento de Tecnología de la Información

- ✗ **A)** opciones A y B
- ✗ **B)** opción e
- ✓ **C)** Opciones B y D
- ✗ **D)** opción A
- ✗ **E)** opción b
- ✗ **F)** opción c
- ✗ **G)** Opción d
- ✗ **H)** Opciones C y E

Explicación

El departamento de Relaciones Públicas y el gobierno federal no deben ser parte del equipo de respuesta a incidentes que investiga un delito que involucra a un empleado interno.

El equipo de respuesta a incidentes debe incluir los siguientes miembros:

- Representante del departamento de Recursos Humanos (HR), porque el representante conoce las reglas que protegen y procesan a un empleado. RRHH siempre debe estar involucrado si un empleado es sospechoso de irregularidades.
- Representante de la alta dirección, porque la acción final contra el empleado sospechoso será tomada por la dirección
- Un representante del departamento de TI para proporcionar evidencia contra el empleado sospechoso si es necesario

Objetivo:
Operaciones de seguridad

Subobsecución: Llevar
a cabo la gestión de incidentes

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, equipo de respuesta a incidentes e investigaciones de incidentes

---

Pregunta #90 de 163

Id. de pregunta: 1105491

Como jefe de departamento de TI, debe garantizar una alta disponibilidad y rendimiento para la red de su organización. También debe asegurarse de que la red es segura. ¿Cuál es la relación entre el rendimiento de la red y la seguridad?

- ✗ **A)** Cuando se aumentan los mecanismos de seguridad, no tiene ningún efecto en el rendimiento.
- ✓ **B)** Cuando se aumentan los mecanismos de seguridad, el rendimiento suele disminuir.
- ✗ **C)** La seguridad siempre debe tener una prioridad más alta que el rendimiento.
- ✗ **D)** Cuando se aumentan los mecanismos de seguridad, el rendimiento suele aumentar.

Explicación

Cuando usted aumenta los mecanismos de seguridad en la red, el funcionamiento de la red disminuye generalmente.

Ninguna de las otras afirmaciones es cierta con respecto a la relación entre el rendimiento de la red y la seguridad. Una organización debe determinar cuándo se debe dar mayor prioridad a la seguridad o al rendimiento.

Los roles de administrador de seguridad y administrador de red deben asignarse a dos personas diferentes. La jerarquía dentro de una organización debe asegurarse de que el administrador de seguridad está bajo una cadena de comando diferente que el administrador de red. Esto garantiza que la seguridad no se omite ni se le asigna una prioridad inferior al rendimiento.

Objetivo:
Operaciones de seguridad

Subobsecución:
Operar y mantener medidas detectivescas y preventivas

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, activos de información

---

Pregunta #91 de 163

Id. de pregunta: 1105420

Durante una investigación reciente de una brecha de seguridad de la red, el equipo de respuesta a incidentes reunió pruebas de oídas. ¿Qué afirmación es cierta de este tipo de evidencia?

- ✓ **A)** Las pruebas de oídas no siempre son admisibles en el tribunal de justicia.
- ✗ **B)** Las pruebas de oídas sólo se refieren a las pruebas orales.

✗ **C)** Las pruebas de oídas se consideran suficientes para procesar a un sospechoso.

✗ **D)** La evidencia de oídas es siempre una prueba de primera mano de información confiable.

Explicación

Las pruebas de oídas no siempre son admisibles en el tribunal de justicia. Puede presentarse ante el tribunal de justicia como prueba admisible sólo si hay una prueba de primera mano de la exactitud y fiabilidad de las pruebas. Por ejemplo, los documentos generados mediante procedimientos ordinarios en el curso ordinario de los negocios son admisibles ante los tribunales de justicia. Los documentos especialmente generados para ser presentados en un tribunal se consideran de oídas y de segunda mano en la naturaleza porque no llevan ninguna prueba de primera mano de la fiabilidad, exactitud y suficiencia. La evidencia de oídas actúa como evidencia de segunda mano para apoyar la información presentada como evidencia en el tribunal de justicia.

Las pruebas de oídas pueden pertenecer tanto a pruebas orales como escritas y no solo a pruebas orales.

Las pruebas de oídas no son suficientes para procesar a un sospechoso ante el tribunal de justicia. Requiere la asistencia de otros tipos de pruebas, como pruebas reales o pruebas concluyentes. Es más probable que las pruebas de oídas se permitan como pruebas en la corte si los registros se recopilan en o cerca del momento en que se aparición del acto que se está investigando. Esperar hasta que pase el tiempo puede perjudicar la admisibilidad de las pruebas de oídas. Los registros que están bajo la custodia de un testigo de forma regular también tienen más probabilidades de ser permitidos como evidencia de oídas.

Los discos se consideran evidencia de oídas porque son sólo copias de la evidencia original. Sin embargo, las pruebas generadas por computadora, como los registros de auditoría y los registros de eventos, se consideran pruebas de segunda mano, no pruebas de oídas.

La evidencia informática debe probar un hecho que sea material para el caso. Su fiabilidad debe ser probada.

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender los requisitos para los tipos de investigación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, evidencia de oídas

---

Pregunta #92 de 163

Id. de pregunta: 1114774

¿Qué elementos NO complementan un sistema de detección de intrusiones (IDS)?

a. sistema de análisis de vulnerabilidades

b. sensores

c. honeypots

d. Celdas acolchadas

e. Software de monitoreo centralizado

- ✗ **A)** Opción d
- ✗ **B)** opción A
- ✗ **C)** opción c
- ✗ **D)** opción e
- ✗ **E)** Opciones C y D
- ✗ **F)** opciones A y B
- ✓ **G)** opciones B y E
- ✗ **H)** opción b

Explicación

Las siguientes entidades complementan el sistema de detección de intrusiones (IDS):

- Sistema de Análisis de Vulnerabilidades (VAS): Identifica vulnerabilidades técnicas en equipos y redes para medir la efectividad de las políticas de seguridad
- Honeypots: Una trampa colocada para detectar, desviar o contrarrestar los intentos de uso no autorizado de los sistemas de información.
- Celdas acolchadas: Restrinja al intruso a un entorno simulado para evitar cualquier daño a la red
- Comprobaciones de integridad de archivos: emplee sumas de comprobación criptográficas para comparar los archivos críticos con los valores de referencia

Los sensores y el software de monitoreo centralizado son en realidad componentes primarios de cualquier IDS y no complementan el IDS. Un sensor detecta eventos anormales mediante la recopilación de datos y su reenvío al software centralizado, que a su vez analiza los datos recopilados en busca de cualquier intento de intrusión o amenaza maliciosa.

Objetivo:
Operaciones de seguridad

Subobsecución:
Llevar a cabo actividades de registro y vigilancia

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 4: Comunicación y Seguridad de red, IDS

Pregunta #93 de 163

Id. de pregunta: 1105467

¿Qué instrucción describe mejor un control de dos hombres?

- ✗ **A)** Un operador controla más de una posición dentro de una organización.
- ✗ **B)** Las responsabilidades de un usuario de equipo y un administrador del sistema están segregadas.
- ✓ **C)** Dos operadores revisan y aprueban el trabajo del otro.
- ✗ **D)** Dos operadores trabajan juntos para completar una tarea determinada.

Explicación

Un control de dos hombres implica que dos operadores revisan y aprueban el trabajo del otro. Un control de dos hombres reduce las posibilidades de fraude. Por lo tanto, se minimiza el riesgo asociado con las operaciones que implican información altamente confidencial.

Un control dual implica que dos operadores trabajan juntos para realizar una tarea y reducir cualquier riesgo asociado con el engaño. El doble control se basa en la premisa de que ambas partes deben estar en connivencia para cometer una violación.

La rotación de puestos de trabajo implica que un empleado puede llevar a cabo las tareas de otro empleado dentro de la organización. En un entorno en el que se utiliza la rotación de puestos de trabajo, un individuo puede cumplir las tareas de más de un puesto en la organización. Esto mantiene un control sobre la actividad de los empleados, proporciona un recurso de copia de seguridad y disuade posibles fraudes.

Las vacaciones obligatorias son controles administrativos que aseguran que los empleados tomen vacaciones a intervalos periódicos. Este procedimiento resulta útil en la detección de actividades sospechosas porque el empleado de reemplazo puede averiguar si el empleado de vacaciones se ha entregado a actividades fraudulentas o no.

La segregación de las funciones de un usuario de equipo y un administrador de sistemas es un ejemplo de segregación de funciones. La segregación de funciones garantiza que no se confíe demasiado en una persona en particular para una tarea delicada. Implica que una actividad sensible se segrega en múltiples actividades y que las tareas se asignan a diferentes individuos para lograr un objetivo común. Una distinción clara entre los deberes de los individuos previene los actos fraudulentos porque la colusión es necesaria para que se produzca una violación. En un entorno adecuadamente segregado, el desarrollo y el mantenimiento de sistemas son compatibles.

Objetivo:
Operaciones de seguridad

Subobsecución:

Comprender y aplicar conceptos fundamentales de operaciones de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, control de dos personas

---

Pregunta #94 de 163

Id. de pregunta: 1111780

¿En qué momento se debe agregar un cambio de configuración al registro de cambios?

- ✗ **A)** Una vez implementado el cambio
- ✗ **B)** Después de probar el cambio
- ✓ **C)** Una vez aprobado el cambio
- ✗ **D)** Una vez solicitado el cambio

Explicación

Se debe agregar un cambio de configuración al registro de cambios una vez aprobado el cambio. El proceso de control de cambios incluye los siguientes pasos:

1. Haga una solicitud formal.
2. Analizar la solicitud. Este paso incluye el desarrollo de la estrategia de implementación, el cálculo de los costos de la implementación y la revisión de las implicaciones de seguridad de la implementación del cambio.
3. Registre la solicitud de cambio.
4. Envíe la solicitud de cambio para su aprobación. Este paso implica obtener la aprobación del cambio real una vez que se ha analizado todo el trabajo necesario para completar el cambio.
5. Realice cambios. Los cambios se implementan y la versión se actualiza en este paso.
6. Enviar los resultados a la administración: en este paso, los resultados del cambio se notifican a la administración para su revisión.

Tenga en cuenta que el CCB no implementa realmente todos los cambios, pero sus miembros son responsables de aprobar todos los cambios. Además, el CCB no es responsable de documentar el cambio. El CCB debe reunirse periódicamente para discutir los informes contables de estado de cambio. La CCB es responsable de asegurar que los cambios realizados no pongan en peligro la solidez del sistema de verificación. El CCB asegura que los cambios realizados son aprobados, probados, documentados e implementados correctamente.

Hay muchos cambios realizados en un sistema que requerirán actualizaciones de documentación, incluidos los siguientes:

- Reconfiguración de un servidor
- Un cambio en la política de seguridad

- La instalación de una revisión en un servidor de producción

Sin embargo, algunos cambios de rutina, incluidas las actualizaciones de firmas de virus, no requerirán actualizaciones de documentación.

Objetivo:
Operaciones de seguridad

Subobsecución:
aprovisionamiento seguro de recursos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, gestión de la configuración

---

Pregunta #95 de 163

Id. de pregunta: 1105410

¿Qué tipo de prueba negará la necesidad de presunciones en el tribunal de justicia?

✗ **A)** evidencia corroborativa
✓ **B)** evidencia directa
✗ **C)** evidencia secundaria
✗ **D)** pruebas de oídas

Explicación

Las pruebas directas negarán la necesidad de presunciones en los tribunales de justicia. La evidencia directa no requiere información de respaldo para probar un hecho. Por lo tanto, no se requieren presunciones. El testimonio de un testigo es un ejemplo de prueba directa porque el testimonio oral de un testigo no requiere ninguna prueba corroborativa para probar el hecho. Otro ejemplo de prueba directa es la copia original de un documento contractual.

La evidencia de oídas se refiere a la evidencia que no tiene prueba de exactitud y confiabilidad. Por ejemplo, un testigo que proporciona testimonio oral basado en lo que esa persona ha escuchado de otra persona será evidencia de oídas. Los documentos generados por computadora también constituyen pruebas de oídas porque es difícil detectar la manipulación de electrones. Los documentos generados por ordenador se pueden modificar fácilmente. Esto se debe a que es difícil detectar si los documentos generados por computadora han sido manipulados o no.

La evidencia secundaria no se considera confiable en el tribunal de justicia, pero resulta útil para establecer un hecho si hay una falta de evidencia real o mejor. Un ejemplo de evidencia secundaria es una copia de un documento original.

La evidencia corroborativa le permite probar un punto o una idea. La evidencia corroborativa es evidencia adicional que es creíble y admisible en el tribunal de justicia. Las pruebas corroborativas no son suficientes para implicar a un

sospechoso, pero pueden complementar las pruebas primarias para establecer el hecho.

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender los requisitos para los tipos de investigación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, evidencia directa

---

Pregunta #96 de 163

Id. de pregunta: 1105412

Para investigar delitos informáticos, ¿con qué agencia trabaja el FBI?

✗ **A)** Interpol y NSA
✗ **B)** Cia y Comisión Europea
✗ **C)** Departamento de Defensa
✓ **D)** Servicio Secreto y aplicación de la ley local

Explicación

Para identificar y procesar a los ciberdelincuentes y establecer la fuente del ataque y la cadena de custodia, el FBI trabaja en coordinación con el Servicio Secreto y la policía local.

El Departamento de Defensa (DoD) controla el ejército de los Estados Unidos y coordina sus actividades. El Departamento de Desarrollo no investiga delitos informáticos.

La principal tarea de la Interpol en materia de delitos cibernéticos es distribuir información sobre delitos transfronterizos e información a los organismos encargados de hacer cumplir la ley de diversos países sobre los últimos acontecimientos.

La Agencia de Seguridad Nacional (NSA) es oficialmente responsable de la seguridad dentro de los Estados Unidos, pero se ocupa principalmente de la inteligencia de señales y la criptografía y tiene una configuración extremadamente sofisticada que consiste en hardware, software y dispositivos.

El objetivo principal de la Agencia Central de Inteligencia (CIA) es preservar la seguridad nacional de los Estados Unidos y las vidas de los estadounidenses. La CIA se ocupa de la seguridad nacional en general. La Comisión Europea no investiga los delitos cibernéticos, pero presenta propuestas y programas para prevenir la ciberdelincuencia a los miembros del consejo de la Unión Europea (UE) y cubre aspectos, como los ataques de denegación de servicio y el comercio electrónico.

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender los requisitos para los tipos de investigación

Referencias:

La Misión de Investigación, https://www.secretservice.gov/investigation/

Pregunta #97 de 163

Id. de pregunta: 1114001

¿Qué se entiende por MTBF?

- ✗ **A)** la cantidad estimada de tiempo que se tardará en reemplazar un equipo
- ✓ **B)** la cantidad estimada de tiempo que un equipo debe permanecer operativo antes de la falla
- ✗ **C)** la cantidad estimada de tiempo que se tardará en reparar un equipo cuando se produzca un fallo
- ✗ **D)** la cantidad estimada de tiempo que se utilizará un equipo antes de que deba reemplazarse

Explicación

El tiempo medio entre fallos (MTBF) es la cantidad estimada de tiempo que un equipo debe permanecer operativo antes del fallo. El MTBF normalmente es suministrado por el proveedor de hardware o un tercero.

El tiempo medio para reparar (MTTR) es la cantidad de tiempo que se tardará en reparar una pieza de equipo cuando se produce una falla.

Ninguna de las otras opciones es correcta.

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender y aplicar conceptos fundamentales de operaciones de seguridad

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 7: Operaciones de Seguridad, MTBF y MTTR

Pregunta #98 de 163

Id. de pregunta: 1192966

Coincide con las descripciones de la izquierda con los tipos de malware a la derecha.

{UCMS id=5736282464452608 type=Activity}

Explicación

Los tipos de malware deben coincidir con las descripciones de la siguiente manera:

- Puerta trasera : un enlace de desarrollador en un sistema o aplicación que permite a los desarrolladores eludir la autenticación normal
- Bomba lógica - un programa que se ejecuta cuando se produce un determinado evento predefinido
- Spyware - un programa que monitorea y rastrea las actividades del usuario
- Caballo de Troya - un programa que infecta un sistema bajo la apariencia de otro programa legítimo

Objetivo:
Operaciones de seguridad

Subobsecución:
Operar y mantener medidas detectivescas y preventivas

Referencias:

Cissp Cert Guide (3ª Edición), Glosario

Pregunta #99 de 163

Id. de pregunta: 1111789

Como parte del equipo de respuesta a incidentes, se le ha entregado un documento de procedimientos que identifica los pasos que debe completar durante una investigación forense.

¿Cuándo se debe completar el paso de recolección de evidencia?

✗ **A)** después de que la evidencia se haya conservado solamente

✓ **B)** después de que se haya identificado el incidente y se hayan conservado las pruebas

✗ **C)** Sólo después de que se haya identificado el incidente

✗ **D)** después de que se ha identificado el incidente, la evidencia se ha conservado, y la evidencia ha sido analizada

Explicación

Debe completar el paso de recopilación de evidencia después de que se haya identificado el incidente y se haya conservado la evidencia.

Los pasos apropiados en una investigación forense son los siguientes:

1. Identificación: este paso puede incluir la detección de eventos/delitos, la resolución de firmas, la detección de perfiles, la detección de anomalías, la recepción de quejas, la supervisión del sistema y el análisis de auditoría.
2. Preservación : este paso puede incluir tecnologías de imágenes, estándares de cadena de custodia y sincronización de tiempo.
3. Recopilación: este paso puede incluir métodos de recopilación aprobados, software aprobado, hardware aprobado, autoridad legal, muestreo, reducción de datos y técnicas de recuperación.
4. Examen: este paso puede incluir trazabilidad, técnicas de validación, técnicas de filtrado, coincidencia de patrones, detección de datos ocultos y extracción de datos ocultos.
5. Análisis : este paso puede incluir trazabilidad, análisis estadístico, análisis de protocolos, minería de datos y determinación de línea de tiempo.
6. Presentación - Este paso puede incluir documentación, testimonio de expertos, aclaración, declaración de impacto de la misión, contramedidas recomendadas e interpretación estadística.
7. Decisión : este paso puede incluir informes de administración, decisiones judiciales y decisiones internas.

Objetivo:
Operaciones de seguridad

Subobsecución: Llevar
a cabo la gestión de incidentes

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, gestión de respuesta a incidentes

---

Pregunta #100 de 163

Id. de pregunta: 1111774

¿Qué problema se supervisa mejor mediante el registro de la carga de la CPU y el uso de memoria?

✗ **A)** Problema de servidor de seguridad
✗ **B)** problema de seguridad
✗ **C)** problema de uso del tiempo de inactividad
✓ **D)** problema de rendimiento

Explicación

El registro de la carga de la CPU y el uso de memoria se pueden utilizar para supervisar el rendimiento del sistema. El nivel de registro requerido se rige por el requisito y las directivas de la organización. Otros servicios que puede registrar para supervisar el rendimiento del sistema incluyen el uso del disco duro, el uso de la red y los procesos críticos del sistema.

El registro de la carga de la CPU y el uso de memoria no se pueden utilizar para supervisar los problemas del firewall. La CPU y la memoria se pueden supervisar utilizando los contadores % de tiempo de procesador y páginas/seg. Debe registrar los sucesos siguientes para los problemas de firewall:

- reinicio del cortafuegos
- reinicio del proxy
- cambios en el archivo de configuración

El registro de la carga de la CPU y el uso de memoria no se pueden utilizar para supervisar los problemas de seguridad. El nivel de registro necesario se rige por los requisitos y las directivas de seguridad de la organización. Hay muchos servicios y comandos que debe registrar por motivos de seguridad. Éstos incluyen el TFTP, el BOOTP, el SUNRPC, el SNMP, y el uso del comando MOUNT.

El registro de la carga de la CPU y el uso de memoria no mide el uso del tiempo de inactividad. El uso del tiempo de inactividad es el tiempo durante el cual los recursos, como la CPU, permanecen inactivos debido a la falta de instrucciones para ejecutar. Otros contadores tendrían que ser supervisados para esta información.

Objetivo:
Operaciones de seguridad

Subobsecución:
Llevar a cabo actividades de registro y vigilancia

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, protección de recursos

---

Pregunta #101 de 163

Id. de pregunta: 1111771

¿Cuál es el término para el proceso de recopilación, análisis y preservación de evidencia?

- ✓ **A)** cadena de custodia
- ✗ **B)** cadena de evidencia
- ✗ **C)** manejo de incidentes
- ✗ **D)** procedimiento legal

Explicación

La cadena de custodia se refiere a procedimientos formales estrictos y organizados de acuerdo con la ley y las regulaciones legales que rigen la recopilación, el análisis y la preservación de la evidencia antes de que la evidencia se presente en un tribunal de justicia. En los delitos informáticos, la mayoría de las pruebas son de naturaleza electrónica y se conocen como pruebas de oídas. Por lo tanto, es importante que se establezca una cadena de custodia claramente definida para garantizar la fiabilidad y la integridad de las pruebas y para que las pruebas sean admisibles ante el tribunal.

La cadena de custodia garantiza la identidad e integridad de las pruebas desde la etapa de recolección hasta su presentación en el tribunal de justicia. El siguiente procedimiento se utiliza para establecer una cadena de custodia para la presentación de pruebas en un tribunal:

- La evidencia debe recopilarse de la manera predefinida siguiendo procedimientos estrictos y formales e indicando los nombres de las personas que aseguraron la evidencia y la validaron.
- La evidencia debe ser marcada por el oficial investigador mencionando la fecha, la hora y el número de caso respectivo.
- La evidencia se sella en un contenedor y el contenedor se marca de nuevo con la misma información. Se prefiere escribir la información en el sello porque es más fácil detectar cualquier cambio en la evidencia examinando el sello roto o el manipulado.
- La ubicación de la evidencia también está documentada.
- Las pruebas son procesadas y analizadas por expertos técnicos.
- Los registros se mantienen mencionando a las personas que accedieron a la información, la hora en que se accedió a la información y las razones para acceder a la información.
- El abogado acusador presenta las pruebas ante el tribunal para implicar al sospechoso.

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender los requisitos para los tipos de investigación

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 7: Operaciones de Seguridad, Investigaciones Forenses y Digitales

---

Pregunta #102 de 163

Id. de pregunta: 1105533

¿Qué sitio suele tardar más en configurarse cuando es necesario?

✗ **A)** sitio redundante

✗ **B)** sitio cálido

✗ **C)** sitio caliente

✓ **D)** sitio frío

Explicación

Un sitio frío suele tardar más en configurarse cuando es necesario. Un sitio frío solo consiste en una habitación desnuda que generalmente incluye pisos elevados, cableado eléctrico y aire acondicionado, pero no incluye ninguna computadora o equipo de comunicaciones.

Un sitio caliente suele ser fácil de configurar cuando es necesario. Consiste en las mismas cosas en un sitio frío, pero también incluye el equipo informático y de telecomunicaciones requerido por su empresa.

Un sitio caliente suele ser más fácil de configurar que un sitio frío, pero más difícil de configurar que un sitio caliente. Consiste en las mismas cosas que en un sitio frío. También incluye el equipo de telecomunicaciones, pero no el equipo informático.

Un sitio redundante es similar a un sitio caliente en que es fácil de configurar cuando sea necesario. Sin embargo, un sitio redundante es propiedad de la compañía que experimenta el desastre, mientras que un sitio caliente se alquila a otra compañía.

Objetivo:
Operaciones de seguridad

Subobsecución:
Probar planes de recuperación ante desastres (DRP)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, recuperación y estrategias de múltiples sitios

---

Pregunta #103 de 163

Id. de pregunta: 1105507

Su organización está implementando un nuevo servidor de archivos. Se le ha pedido que implemente un subsistema de disco que es un sistema de disco resistente a errores (FRDS).

¿Qué criterio debe cumplir este sistema?

✗ **A)** Protege contra la pérdida de acceso a los datos debido a un corte de energía externo.

✗ **B)** Protege contra la pérdida de acceso a los datos debido a fallas en la fuente de alimentación.

✗ **C)** Protege contra la pérdida de datos debido a un corte de energía externo.

✓ **D)** Protege contra la pérdida de datos debido a fallas en la unidad de disco.

Explicación

Un sistema de disco resistente a fallos (FRDS) protege contra la pérdida de datos debido a un fallo de la unidad de disco. La función básica de un FRDS es proteger los servidores de archivos de la pérdida de datos y una pérdida de disponibilidad debido a un error de disco.

Un sistema de disco tolerante a fallos (FTDS) protege contra la pérdida de datos debido a un fallo de alimentación externo y la pérdida de acceso a los datos debido a un fallo en la fuente de alimentación.

Un sistema de disco tolerante a desastres (DTDS) protege contra la pérdida de acceso a los datos debido a un fallo en la fuente de alimentación.

Objetivo:
Operaciones de seguridad

Subobsecución:
Implementar estrategias de recuperación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y gestión de riesgos, tolerancia a fallos

---

Pregunta #104 de 163

Id. de pregunta: 1105405

¿Qué parte de un sistema informático debe ser inspeccionada en busca de archivos y datos ocultos?

✗ **A)** espacio de bits

✗ **B)** espacio reducido

✗ **C)** espacio de custodia

✓ **D)** espacio de holgura

Explicación

El espacio de holgura de un sistema informático debe inspeccionarse en busca de archivos o datos ocultos. Una imagen de un disco duro conserva tanto los datos en vivo como la información atrapada en el espacio de holgura y otros escondites. El espacio de holgura hace referencia a un espacio no utilizado en un clúster de discos.

El espacio de bits, el espacio de custodia y el espacio reducido son términos no válidos con referencia al examen forense de un sistema informático como parte de la respuesta a incidentes.

En muchos sistemas operativos, como Windows, un clúster completo se reserva para un archivo incluso si los datos reales que se almacenan requieren menos almacenamiento que el tamaño del clúster. Esto se debe a que los sistemas operativos almacenan información en clústeres de tamaño fijo. El espacio no utilizado en un clúster se denomina espacio de holgura. El proceso normal de eliminación de archivos no elimina los archivos, sino sólo los punteros a ella. Por lo tanto, los datos antiguos se conservan en el espacio de holgura hasta que se sobrescriben físicamente.

En los medios de almacenamiento, como las cintas, donde los datos magnéticos no se borran hasta que se sobrescriben con nuevos datos, no hay posibilidad de un espacio de holgura.

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender y apoyar las investigaciones

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, análisis de medios

---

Pregunta #105 de 163

Id. de pregunta: 1105492

Acaba de recibir una alerta de que se ha detectado un intento de intrusión en la red. Es necesario lanzar las contramedidas iniciales para este ataque. ¿Qué acción NO se recomienda como contramedida inicial?

- ✗ **A)** Realizar las actividades necesarias para contener la intrusión.
- ✗ **B)** Notifique al equipo de respuesta a incidentes.
- ✓ **C)** Lanzar un contraataque contra el intruso.
- ✗ **D)** Configure el IDS para caer los paquetes que son malévolos en naturaleza.

Explicación

El lanzamiento de contraataques contra el sistema del intruso no se recomienda como contramedida inicial.

El primer paso debe ser contener la intrusión. El IDS debe configurarse para enviar la notificación de eventos al miembro designado del equipo de respuesta a incidentes. Después de la notificación, el equipo de respuesta a incidentes puede tomar las medidas adecuadas para contener la intrusión. El IDS se puede también configurar para caer los paquetes de red que aparecen ser malévolos en naturaleza. Por ejemplo, el IDS puede caer los paquetes con los mismos IP Addresses de origen y de destino, indicando un ataque de la TIERRA. Otras acciones posibles son recopilar información adicional sobre el ataque y reconfigurar los sistemas internos para protegerlos contra futuros ataques del atacante.

Objetivo:
Operaciones de seguridad

Subobsecución:
Operar y mantener medidas detectivescas y preventivas

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 7: Operaciones de seguridad, detección de intrusiones y prevención

---

Pregunta #106 de 163

Id. de pregunta: 1105440

Al examinar los informes de rendimiento de los recursos de la organización, observa un aumento significativo del rendimiento en el servidor de archivos de la organización. El registro del servidor indica que se actualizaron la memoria y el disco duro del servidor de archivos. Como miembro del equipo de operaciones, ¿qué debe hacer?

- ✗ **A)** Continúe supervisando el rendimiento del servidor de archivos.
- ✗ **B)** Investigue el aumento del rendimiento del servidor de archivos.
- ✗ **C)** Diagnostique el aumento del rendimiento del servidor de archivos.
- ✓ **D)** Cree una nueva línea base de rendimiento para el servidor de archivos.

Explicación

Debe crear una nueva línea base de rendimiento para el servidor de archivos. El equipo de operaciones siempre debe examinar cualquier desviación de los estándares establecidos.

No debe investigar el aumento del rendimiento del servidor de archivos ni diagnosticar el aumento del rendimiento del servidor de archivos. Dado que se ha actualizado el hardware del servidor de archivos, conoce la causa del aumento del rendimiento. El equipo de operaciones solo debe investigar sucesos inusuales o inexplicables. Después de la investigación inicial de los sucesos inusuales o inexplicables, el equipo de operaciones debe diagnosticar el suceso.

No debe seguir supervisando el rendimiento del servidor de archivos hasta que cree una nueva línea base de rendimiento para el servidor de archivos. Una vez establecida la nueva línea base, puede seguir supervisando el rendimiento del servidor y comparar el rendimiento con la nueva línea base.

Objetivo:
Operaciones de seguridad

Subobsecución:
Llevar a cabo actividades de registro y vigilancia

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 8: Seguridad de desarrollo de software, operar / mantener

---

Pregunta #107 de 163

Id. de pregunta: 1111784

¿Qué funciones NO están asociadas en un entorno correctamente segregado?

- ✓ **A)** autorización de acceso y auditoría
- ✗ **B)** desarrollo de sistemas y mantenimiento de sistemas
- ✗ **C)** entrada de datos y programación de trabajos
- ✗ **D)** administración de seguridad y control de calidad

Explicación

La autorización de acceso y la auditoría no están asociadas en un entorno correctamente segregado. Las aprobaciones para la autorización de acceso otorgadas por un individuo deben ser auditadas por un individuo separado. Esto garantizará la segregación de funciones y actuará como una verificación cruzada para la supervisión de los privilegios asignados. El componente de auditoría del sistema de tecnología de la información debe ser independiente y distinto de la arquitectura de seguridad del sistema de información de un sistema.

Las organizaciones siguen la política de separación de funciones por las siguientes razones:

- Las tareas de alta seguridad se distribuyen entre los individuos para garantizar que la seguridad de la organización no se asigna a un solo individuo desde el principio de una tarea hasta el final.
- En el caso de una brecha de seguridad o un fraude, se hace más fácil identificar a la persona que es responsable de la misma. Por lo tanto, la separación de funciones establece la rendición de cuentas.
- También se reducen las posibilidades de un error o un error durante la finalización de la tarea. Esto se debe a que diferentes individuos que trabajan en subtareas separadas actúan como una comprobación cruzada entre sí.

Por ejemplo, un programador de software involucrado en el desarrollo de código no es responsable de las pruebas. Las pruebas en el código desarrollado por el programador deben ser realizadas por un individuo separado o un equipo para informar de errores y modificaciones. Este proceso proporciona una comprobación cruzada de una tarea confidencial dividiéndola en varias subtareas.

Ejemplos de funciones que son compatibles en un entorno correctamente segregado son los siguientes:

- Entrada de datos y programación de trabajos
- Administración de la seguridad y garantía de calidad
- Desarrollo y mantenimiento de sistemas

Objetivo:

Operaciones de seguridad

Subobsecución:

Comprender y aplicar conceptos fundamentales de operaciones de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, separación de funciones

---

Pregunta #108 de 163

Id. de pregunta: 1105512

Su empresa tiene una solución de copia de seguridad que realiza una copia de seguridad completa cada sábado por la noche y una copia de seguridad incremental todas las demás noches. Un sistema vital se estrella el lunes por la mañana. ¿Cuántas copias de seguridad se necesitarán restaurar?

- ✓ **A)** Dos
- ✗ **B)** Uno
- ✗ **C)** Cuatro
- ✗ **D)** Tres

Explicación

Debido a que el sistema se bloquea el lunes por la mañana, deberá restaurar dos copias de seguridad: la copia de seguridad completa del sábado por la noche y la copia de seguridad incremental del domingo por la noche. Cuando se incluyen copias de seguridad incrementales en el plan de copia de seguridad, deberá restaurar la copia de seguridad completa y todas las copias de seguridad incrementales que se han realizado desde la copia de seguridad completa. Dado que el error se produjo el lunes por la mañana, solo es necesario restaurar la copia de seguridad completa del sábado y la copia de seguridad incremental del domingo.

Si el bloqueo se hubiera producido el martes por la mañana, habría tenido que restaurar tres copias de seguridad: la copia de seguridad completa del sábado por la noche, la copia de seguridad incremental del domingo por la noche y la copia de seguridad incremental del lunes por la noche.

Si el bloqueo se hubiera producido el miércoles por la mañana, habría necesitado restaurar cuatro copias de seguridad: la copia de seguridad completa del sábado por la noche, la copia de seguridad incremental del domingo por la noche, la copia de seguridad incremental del lunes por la noche y la copia de seguridad incremental del martes por la noche.

Objetivo:

Operaciones de seguridad

Subobsecución:

Implementar estrategias de recuperación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, tipos de copia de seguridad de datos y esquemas

---

Pregunta #109 de 163

Id. de pregunta: 1111781

¿Qué proceso incluye la auditoría y el seguimiento de los cambios realizados en la base informática de confianza?

- ✓ **A)** administración de la configuración
- ✗ **B)** controles de entrada y salida
- ✗ **C)** controles multimedia
- ✗ **D)** controles del sistema

Explicación

La administración de la configuración identifica los controles y los cambios de auditoría realizados en la base informática de confianza. Los cambios de auditoría incluyen cambios realizados en las configuraciones de hardware, software y firmware a lo largo del ciclo de vida de los activos de infraestructura. La administración de la configuración garantiza que los cambios en la infraestructura se realizarán de forma controlada siguiendo un enfoque de proceso. También garantiza que los cambios futuros no infrinjan la directiva de seguridad y los objetivos de seguridad de una organización.

El proceso de administración de la configuración implica la aprobación y autorización adecuadas, las pruebas, la implementación y la documentación de los cambios que han tenido lugar en la infraestructura. Todos los cambios realizados en la infraestructura están sujetos a auditorías y revisiones para garantizar el cumplimiento de la política de seguridad. La administración de la configuración implica la captura de información y el control de versiones. La administración de la configuración informa del estado del procesamiento de cambios. La administración de la configuración documenta las características funcionales y físicas de cada elemento de configuración. Los cuatro aspectos principales de la administración de la configuración son:

- Identificación de la configuración
- Control de configuración
- Contabilidad de estado de configuración
- Auditoría de configuración

Los controles de medios garantizan que la confidencialidad, integridad y disponibilidad de los datos almacenados en los medios de almacenamiento se cumplan correctamente y no se vean comprometidas. Los controles de medios definen los controles adecuados para el etiquetado, la manipulación, el almacenamiento y la eliminación de medios de almacenamiento. No tienen nada que ver con la base informática de confianza. Debe tener en cuenta los siguientes controles multimedia:

- Los medios de datos deben efectuarse para proporcionar un control de inventario físico.
- Todos los medios de almacenamiento de datos deben estar marcados con precisión.
- Se debe proporcionar un entorno de almacenamiento adecuado para los medios.

Los controles del sistema restringen la ejecución de instrucciones que sólo se pueden ejecutar cuando un sistema operativo se ejecuta en el supervisor o en el modo privilegiado. Los controles del sistema forman parte de la arquitectura del sistema operativo. El tipo de instrucciones que se pueden ejecutar en un determinado nivel se define mediante la arquitectura del sistema operativo mediante las tablas de control del sistema operativo.

Controlar la entrada y salida de un sistema implica programar una aplicación para que acepte solo valores restringidos y específicos como entradas. Esto evita errores y mal uso mediante la manipulación de los valores de entrada. Para lograr el propósito de generar resultados, una aplicación solo debe aceptar valores legítimos. Por ejemplo, un paquete de contabilidad diseñado para realizar cálculos no debe aceptar caracteres alfabéticos como valores de entrada.

La identificación de la configuración implica el uso de elementos de configuración (SI). Un CI es un subconjunto identificable de forma única del sistema que representa la parte más pequeña que está sujeta a procedimientos de control de configuración independientes. Los CIs pueden variar ampliamente en tamaño, tipo y complejidad.

Objetivo:
Operaciones de seguridad

Subobsecución:
aprovisionamiento seguro de recursos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, gestión de la configuración

---

Pregunta #110 de 163

Id. de pregunta: 1114786

¿Cuáles son los principales tipos de cerraduras mecánicas?

a. Bloqueos combinados

b. Bloqueos de cifrado

c. cerraduras de tutela

d. Cerraduras del vaso

- ✗ **A)** opción A
- ✓ **B)** Opciones C y D
- ✗ **C)** opción b
- ✗ **D)** opción c
- ✗ **E)** opciones A y B
- ✗ **F)** Opción d

Explicación

Los dos tipos principales de cerraduras mecánicas son cerraduras de la salada y cerraduras del vaso.

Las cerraduras con warded son candados básicos. La cerradura tiene salas (proyecciones de metal alrededor del ojo de la cerradura), y sólo una llave en particular trabajará con las salas para desbloquear la cerradura.

Una cerradura de vaso tiene más piezas que una cerradura de caja. La llave cabe en el cilindro, elevando las piezas de la cerradura a la altura correcta. Hay tres tipos de cerraduras de vaso: cerraduras de vaso de alfiler, cerraduras de vaso de oblea y cerraduras de vaso de nivel.

Los bloqueos combinados requieren la combinación correcta de números para desbloquear. Las cerraduras combinadas no se consideran cerraduras mecánicas según (ISC)2.

Los bloqueos de cifrado son programables y utilizan teclados para controlar el acceso. Se debe introducir una combinación específica.

Objetivo:
Operaciones de seguridad

Subobjetiva:
Implementar y administrar la seguridad física

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Cerraduras

---

Pregunta #111 de 163

Id. de pregunta: 1105501

¿Qué tipo de actualización realiza reparaciones en un equipo durante su funcionamiento normal para que el equipo pueda seguir funcionando hasta que se pueda realizar una reparación permanente?

- ✗ **A)** parche

✗ **B)** Service Pack

✓ **C)** revisión

✗ **D)** paquete de soporte técnico

Explicación

Una revisión realiza reparaciones en un equipo durante su funcionamiento normal para que el equipo puede seguir funcionando hasta que se puede realizar una reparación permanente. Por lo general, implica la sustitución de archivos con una versión actualizada. Una revisión también puede denominarse corrección de errores.

Un service pack o support pack es un conjunto completo de correcciones combinadas en un solo producto. Los Service Packs generalmente incluyen todas las revisiones y revisiones. Un paquete de soporte técnico es otro término que se usa para los Service Pack.

Los parches son correcciones temporales de un programa. Una vez que se conocen más datos acerca de un problema, se puede emitir un service pack o revisión para corregir el problema a mayor escala.

Objetivo:
Operaciones de seguridad

Subobsecución:
Implementar y apoyar la gestión de parches y vulnerabilidades

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, sistemas basados en el cliente

---

Pregunta #112 de 163

Id. de pregunta: 1105528

Durante el análisis de impacto en el negocio (BIA), el comité de continuidad del negocio identifica un servidor que tiene un tiempo de inactividad máximo tolerable (MTD) de 48 horas. ¿En qué categoría de tiempo de inactividad máximo tolerable (MTD) debe colocarse este sistema?

✓ **A)** importante

✗ **B)** crítico

✗ **C)** accidental

✗ **D)** normal

✗ **E)** urgente

Explicación

Un sistema entraría en la categoría de tiempo de inactividad tolerable máximo (MTD) importante si necesitara ser restaurado dentro de las 72 horas o menos.

Un sistema crítico tendría que ser restaurado en menos de 24 horas. Un sistema urgente tendría que ser restaurado en un plazo de 24 horas. Un sistema normal tendría que ser restaurado dentro de 7 días. Un sistema no esencial tendría que ser restaurado en 30 días.

Objetivo:
Operaciones de seguridad

Subobsecución:
Implementar procesos de recuperación ante desastres (DR)

Referencias:

CISSP Cert Guide (3rd Edition) Chapter 7 Security Operations MTBF and MTTR

Pregunta #113 de 163

Id. de pregunta: 1114778

Como parte de la nueva iniciativa de seguridad de su organización, debe asegurarse de que todos los sistemas están reforzados. ¿Qué debes hacer?

un. Quite todas las aplicaciones innecesarias.

B. Quite o deshabilite todos los servicios innecesarios.

c. Configurar los servicios de aplicación para que usen la misma cuenta sin privilegios.

d. Configurar los servicios de base de datos para que usen una cuenta sin privilegios.

- ✗ **A)** opción c
- ✗ **B)** Opción d
- ✗ **C)** opciones a, b y c
- ✗ **D)** opción b
- ✓ **E)** opciones a, b y d
- ✗ **F)** opción A
- ✗ **G)** todas las opciones

Explicación

Para reforzar un sistema, debe completar los pasos siguientes:

- Quite todas las aplicaciones innecesarias.
- Quite o deshabilite todos los servicios innecesarios.
- Configure los servicios de base de datos para utilizar una cuenta sin privilegios.
- Configure cada servicio de aplicación para que use su propia cuenta sin privilegios.

Los servicios de aplicación no deben utilizar la misma cuenta sin privilegios. Debe utilizar una cuenta única para cada servicio. Si lo hace, un compromiso de la cuenta de un servicio no concede acceso a otros servicios del sistema.

Objetivo:
Operaciones de seguridad

Subobjecución:
Aplicar técnicas de protección de recursos

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 7: Operaciones de seguridad, endurecimiento del sistema

---

Pregunta #114 de 163

Id. de pregunta: 1105419

Durante una investigación forense reciente, varios resúmenes del mensaje fueron obtenidos. ¿Cuál es la principal desventaja de usar esta evidencia?

✓ **A)** marca de tiempo modificada
✗ **B)** autenticación estricta
✗ **C)** tiempo de acceso más lento
✗ **D)** procesamiento más rápido

Explicación

La principal desventaja de los resúmenes de mensajes es que se puede modificar la marca de tiempo. Durante el transcurso de una investigación forense, la hora de último acceso para un archivo se cambia cuando se crea un resumen del mensaje en los datos recopilados. Los resúmenes de los mensajes son necesarios para garantizar que las pruebas no se manipulen durante el curso de la investigación. Una marca de tiempo de registro se cambia debido a que se está llevando a cabo una transacción y sobrescribe la marca de tiempo del incidente que se produjo originalmente.

Una síntesis del mensaje es una salida fija creada mediante una función hash unidireccional. Un resumen del mensaje se crea a partir de un conjunto variable de entrada, también denominado suma de comprobación. Un resumen del mensaje es útil para detectar si se realiza algún cambio en los registros durante el transcurso de la cadena de custodia. Se espera que la síntesis del mensaje sea menor que la cadena de datos original.

Los resúmenes de mensajes no proporcionan una autenticación estricta y se ocupan de la integridad de la información.

Los resúmenes de mensajes no contribuyen a un mayor tiempo de procesamiento ni a un tiempo de acceso más lento.

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender los requisitos para los tipos de investigación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, preservar y recopilar evidencia

---

Pregunta #115 de 163

Id. de pregunta: 1105463

¿Qué acuerdo le permite identificar actividades fraudulentas al permitir que un empleado desempeñe más de un rol en la organización?

- ✗ **A)** separación de funciones
- ✓ **B)** rotación de trabajos
- ✗ **C)** control dual
- ✗ **D)** vacaciones obligatorias

Explicación

La rotación de puestos de trabajo implica la rotación de tareas y puede ayudar a identificar actividades fraudulentas. La rotación de puestos de trabajo implica que un empleado puede llevar a cabo las tareas de otro empleado dentro de la organización. En un entorno en el que se utiliza la rotación de puestos de trabajo, un individuo puede cumplir las tareas de más de un puesto en la organización. Esto mantiene un control sobre las actividades de otros empleados, proporciona un recurso de copia de seguridad y disuade posibles fraudes.

El control dual implica que dos operadores trabajan juntos para realizar una tarea delicada. El control dual puede reducir cualquier riesgo asociado con el engaño. El doble control se basa en la premisa de que ambas partes deben estar en connivencia para cometer una violación.

La segregación de funciones garantiza que no se confíe demasiado en una persona en particular para una tarea delicada. Implica que una actividad sensible se segrega en múltiples actividades y que las tareas se asignan a diferentes individuos para lograr un objetivo común. Una distinción clara entre los deberes de los individuos previene los actos fraudulentos porque la colusión es necesaria para que se produzca una violación.

Las vacaciones obligatorias son controles administrativos que aseguran que los empleados tomen vacaciones a intervalos periódicos. Este procedimiento resulta útil en la detección de actividades sospechosas porque el empleado de reemplazo puede averiguar si el empleado de vacaciones se ha entregado a actividades fraudulentas o no.

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender y aplicar conceptos fundamentales de operaciones de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, rotación de trabajo y vacaciones obligatorias

---

Pregunta #116 de 163

Id. de pregunta: 1114784

El comité de continuidad del negocio ha desarrollado el análisis de impacto en el negocio (BIA), ha identificado los controles preventivos que se pueden implementar y ha desarrollado las estrategias de recuperación. A continuación, el comité debería desarrollar un plan de contingencia.

¿Qué equipos deben incluirse en el desarrollo de este plan para ayudar en la ejecución del plan final?

a. equipo de restauración

b. Equipo de evaluación de daños

c. Equipo de salvamento

d. Equipo de gestión de riesgos

e. Equipo de respuesta a incidentes

- ✗ **A)** opción b
- ✗ **B)** opciones a, d y e
- ✗ **C)** opción e
- ✗ **D)** Opción d
- ✗ **E)** opción A
- ✗ **F)** opción c
- ✓ **G)** opciones a, b y c

Explicación

Los equipos que deben incluirse en el desarrollo del plan de contingencia para ayudar en la ejecución del plan final son los equipos de restauración, evaluación de daños y salvamento. Otros equipos que también deben incluirse son los equipos legales, de relaciones con los medios de comunicación, recuperación de redes, reubicación, seguridad y telecomunicaciones.

El equipo de gestión de riesgos, si bien participa en el desarrollo real del plan de contingencia, generalmente no ayuda en la ejecución del plan final. El equipo de gestión de riesgos ayuda a descubrir los riesgos y decidir la probabilidad de los riesgos.

El equipo de respuesta a incidentes es responsable de gestionar todas las respuestas a incidentes de seguridad. No forman parte de la ejecución de un plan de contingencia. El equipo de respuesta a incidentes es responsable de gestionar todas las respuestas a incidentes de seguridad. No forman parte de la ejecución de un plan de contingencia.

Objetivo:
Operaciones de seguridad

Subobsecución:
Implementar procesos de recuperación ante desastres (DR)

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, Plan de Contingencia

---

Pregunta #117 de 163

Id. de pregunta: 1114776

¿Qué tecnologías se consideran tecnologías de teleobservación?

a) Aeronaves no tripuladas

b) Aeronaves tripuladas

c. Satélites

d. Cámaras terrestres

- ✗ **A)** Opción d
- ✗ **B)** opción b
- ✗ **C)** opción c
- ✗ **D)** opción A
- ✗ **E)** opciones a, b y c
- ✗ **F)** opciones b, c y d
- ✓ **G)** todas las opciones

Explicación

Todas las opciones se consideran tecnologías de teledetección. La teledetección es la adquisición de información utilizando imágenes fotográficas, de radar, infrarrojas o multiespectrales a través de sensores remotos, incluidas aeronaves tripuladas y no tripuladas, buques, satélites y cámaras terrestres remotas. La categoría más crítica de información para capturar inmediatamente después de un desastre es la inteligencia precisa y oportuna sobre el alcance, el alcance y el impacto del evento. Las tecnologías de teledetección también proporcionan vigilancia de la seguridad a regiones geográficas distantes.

Los sistemas de teledetección pueden proporcionar un medio alternativo muy eficaz para reunir información sobre el suceso. La inteligencia de teleobservación (RS) puede integrarse en los sistemas de información geográfica (SIG) para producir productos basados en mapas.

Objetivo:
Operaciones de seguridad

Subobsecución:
Llevar a cabo actividades de registro y vigilancia

Referencias:

Teledetección, https://www.thoughtco.com/an-overview-of-remote-sensing-1434624

Pregunta #118 de 163

Id. de pregunta: 1105432

Está creando una solución de supervisión para la red de su empresa. Defina una regla que impida que un cliente de correo electrónico ejecute el comando cmd.exe y le avise cuando se intente. ¿Qué tipo de monitoreo está utilizando?

✗ **A)** basado en firmas
✗ **B)** basado en la detección de uso indebido
✓ **C)** basado en el comportamiento
✗ **D)** basado en anomalías

Explicación

La supervisión basada en el comportamiento busca un comportamiento que no está permitido o que puede percibirse como malintencionado y actúa en consecuencia. Con este tipo de monitoreo, no es necesario conocer la firma de la acción maliciosa. Además, es posible que el sistema no reconozca que las acciones están fuera de la norma. Cuando se define una regla que impide que un cliente de correo electrónico ejecute el comando cmd.exe y le avisa cuando se intenta, se utiliza la supervisión basada en el comportamiento.

La supervisión basada en la detección de uso indebido es la misma que la supervisión basada en firmas. La supervisión basada en firmas requiere que las actualizaciones se obtengan regularmente para garantizar la eficacia. La supervisión basada en firmas vigila las intrusiones que coinciden con una identidad o firma conocida cuando se comparan con una base de datos que contiene las identidades de posibles ataques. Esta base de datos se conoce como la base de datos de firmas.

La supervisión basada en anomalías detecta cualquier cambio o desviación en el tráfico de red. Con este tipo de monitoreo, hay un período de aprendizaje inicial antes de que se puedan detectar anomalías. Una vez establecidas las líneas de base, la supervisión basada en anomalías puede detectar comportamientos anómalos. A veces, la línea de base se establece a través de un proceso manual.

La supervisión basada en red está conectada a la red en un lugar donde puede supervisar todo el tráfico de red. Implementa respuestas pasivas y activas. Respuestas pasivas que incluyen registro, notificación y rechazo. Las respuestas activas incluyen la terminación de procesos o sesiones, cambios en la configuración de la red y engaño.

Objetivo:
Operaciones de seguridad

Subobsecución:
Llevar a cabo actividades de registro y vigilancia

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Ids de comunicación y seguridad de red

---

Pregunta #119 de 163

Id. de pregunta: 1105464

Ha recibido una lista de usuarios y sus trabajos. Debe implementar el principio de privilegios mínimos. ¿Cuál es el siguiente paso que se debe realizar?

- ✗ **A)** Configure los privilegios adecuados para la cuenta del usuario.
- ✓ **B)** Determine el conjunto mínimo de privilegios necesarios para realizar el trabajo del usuario.
- ✗ **C)** Configure las pertenencias a grupos adecuadas para la cuenta del usuario.
- ✗ **D)** Determine el conjunto máximo de privilegios necesarios para realizar el trabajo del usuario.

Explicación

Después de determinar cuál es el trabajo de un usuario, debe determinar el conjunto mínimo de privilegios necesarios para realizar el trabajo del usuario.

No debe determinar el conjunto máximo de privilegios necesarios para realizar el trabajo del usuario. Esto es contrario al principio de privilegios mínimos. El principio de privilegios mínimos garantiza que se concedan los derechos, permisos y privilegios de usuario más restrictivos.

No puede configurar los privilegios o pertenencias a grupos adecuados para la cuenta del usuario hasta que se haya realizado un análisis de trabajo adecuado. El análisis del trabajo implica determinar cuál es el trabajo de un usuario y determinar el conjunto mínimo de privilegios necesarios para realizar el trabajo del usuario.

Los privilegios excesivos se producen cuando a un usuario se le han concedido más derechos, permisos y privilegios de los que requiere el trabajo del usuario. Cuando esto ocurre, puede tener efectos perjudiciales en la estructura de seguridad de una empresa. En un entorno grande, los privilegios excesivos son difíciles de controlar. Es esencial que se establezcan los procedimientos adecuados para garantizar que el principio de privilegio mínimo se ejecute correctamente.

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender y aplicar conceptos fundamentales de operaciones de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, necesidad de saber / privilegios mínimos

---

Pregunta #120 de 163

Id. de pregunta: 1105409

¿Qué afirmación es cierta de la evidencia circunstancial?

- ✗ **A)** Ayuda a probar un punto o una idea.
- ✗ **B)** Se basa en documentos originales para probar un hecho.
- ✗ **C)** Prueba directamente un hecho y no requiere corroboración.
- ✓ **D)** Requiere inferencia a partir de los hechos de que se tenga acceso.

Explicación

La evidencia circunstancial presenta hechos intermedios que facilitan al juez y al jurado deducir lógicamente un hecho. La evidencia circunstancial es un hecho que se utiliza para deducir otro hecho relacionado con el asunto primario bajo consideración. Un sospechoso no puede ser implicado basándose únicamente en la evidencia circunstancial. Por ejemplo, si un individuo amenaza con entrometerse en la red de la empresa, y la intrusión se produce en los próximos días, la evidencia circunstancial establecerá el punto de que la persona es un sospechoso, pero el individuo no estará implicado.

La evidencia directa prueba directamente un hecho y no requiere el apoyo de otras pruebas para establecer el hecho. La principal diferencia entre la evidencia directa y la evidencia circunstancial es que no se requieren presunciones para la evidencia directa. La evidencia directa prueba o refuta un acto específico a través del testimonio oral basado en la información recopilada a través de los cinco sentidos del testigo.

La evidencia corroborativa le permite probar un punto o una idea. La evidencia corroborativa es evidencia adicional que es creíble y admisible en el tribunal de justicia. Las pruebas corroborativas no son suficientes para implicar a un sospechoso, pero pueden complementar las pruebas primarias para establecer el hecho.

La mejor evidencia se basa en documentos y contratos originales para probar un hecho. La mejor evidencia o la evidencia real es una pieza de evidencia que tiene el más alto grado de confiabilidad.

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender los requisitos para los tipos de investigación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, evidencia circunstancial

---

Pregunta #121 de 163

Pregunta con id.: 1105400

Un empleado es sospechoso de actividad delictiva que implica el acceso a datos en exceso de la autoridad del empleado. Usted ha obtenido la copia original firmada del acuerdo de no derecho a la privacidad que el empleado firmó cuando fue contratado. ¿Qué tipo de evidencia es este acuerdo?

- ✓ **A)** mejor evidencia
- ✗ **B)** pruebas de oídas
- ✗ **C)** evidencia secundaria
- ✗ **D)** evidencia corroborativa

Explicación

El acuerdo de no derecho a la privacidad que el empleado firmó cuando fue contratado es la mejor evidencia. La mejor evidencia proporciona la mayor confiabilidad en un ensayo. Cualquier contrato original firmado se considera la mejor evidencia.

Las pruebas secundarias no son tan fiables para demostrar la inocencia o la culpabilidad. Las pruebas orales o las copias de documentos originales se consideran pruebas secundarias.

La evidencia corroborativa ayuda a probar un punto. Es complementario para ayudar a apoyar la mejor evidencia.

La evidencia de oídas es evidencia oral o escrita que es de segunda mano.

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender y apoyar las investigaciones

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, mejor evidencia

---

Pregunta #122 de 163

Id. de pregunta: 1105448

Recientemente ha sido contratado como administrador de seguridad de su organización. Se le han dado varios informes de seguridad. Uno de los informes muestra información estadística del detector de anomalías de la organización. ¿Cuál es la tarea principal de este sistema?

- ✗ **A)** Para identificar cuellos de botella en segmentos de red
- ✗ **B)** identificar el uso de los recursos de la red y establecer la rendición de cuentas
- ✓ **C)** para identificar la actividad anormal
- ✗ **D)** para identificar la actividad legítima

Explicación

Los detectores de anomalías identifican patrones inusuales y anormales en la actividad de la red mediante la creación de perfiles o modelos en el patrón de comportamiento normal de los usuarios individuales, hosts o conexiones de red. De acuerdo con los datos recogidos con respecto a actividad normal, cualquier desviación estadística del patrón normal del comportamiento se divulga como anomalía. Una de las desventajas de IDS basado en anomalías es que genera falsos positivos porque el patrón de comportamiento puede variar o el patrón de comportamiento es demasiado dinámico para analizarlo correctamente.

Además de la detección de anomalías, la detección de uso indebido también se utiliza para analizar eventos. Los detectores de mal uso también se pueden caracterizar como un IDS basado en firmas.

El IDS basado en firmas se basa en la base de datos de ataques conocidos y sus respectivos patrones.

Cada ataque basado en la red tiene un patrón único y forma una firma única que puede ser rastreada por el IDS para detectar actividad maliciosa. La base de datos de firmas debe actualizarse regularmente para realizar un seguimiento

de los últimos ataques y sus variaciones. Un patrón de tráfico que no califica como firma válida de un ataque se considera actividad normal y es aceptado por el IDS.

Objetivo:
Operaciones de seguridad

Subobsecución:
Llevar a cabo actividades de registro y vigilancia

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 4: Comunicación y Seguridad de red, IDS

Pregunta #123 de 163

Id. de pregunta: 1105430

Se le ha pedido que implemente la supervisión de red que detecta cualquier cambio o desviación en el tráfico de red. Al configurar la supervisión, se establecen líneas de base de tráfico de red. ¿Qué tipo de monitoreo está implementando?

✗ **A)** basado en el comportamiento
✗ **B)** basado en firmas
✓ **C)** basado en anomalías
✗ **D)** basado en red

Explicación

La supervisión basada en anomalías detecta cualquier cambio o desviación en el tráfico de red. Con este tipo de monitoreo, hay un período de aprendizaje inicial antes de que se puedan detectar anomalías. Una vez establecidas las líneas de base, la supervisión basada en anomalías puede detectar actividades anómalas. A veces, la línea de base se establece a través de un proceso manual.

La supervisión basada en red está conectada a la red en un lugar donde puede supervisar todo el tráfico de red. Implementa respuestas pasivas y activas. Las respuestas pasivas incluyen el registro, la notificación y el rechazo. Las respuestas activas incluyen la terminación de procesos o sesiones, cambios en la configuración de la red y engaño.

La supervisión basada en el comportamiento busca un comportamiento que no está permitido y actúa en consecuencia.

La supervisión basada en firmas requiere que las actualizaciones se obtengan regularmente para garantizar la eficacia. La supervisión basada en firmas vigila las intrusiones que coinciden con una identidad o firma conocida

cuando se comparan con una base de datos que contiene las identidades de posibles ataques. Esta base de datos se conoce como la base de datos de firmas.

Objetivo:
Operaciones de seguridad

Subobsecución:
Llevar a cabo actividades de registro y vigilancia

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Ids de comunicación y seguridad de red

---

Pregunta #124 de 163

Id. de pregunta: 1113999

¿Qué tipo de sistema de detección de intrusiones (IDS) es un detector de mal uso?

- ✗ **A)** IDS de control de acceso
- ✗ **B)** IDS basados en el tiempo
- ✓ **C)** IDS basados en firmas
- ✗ **D)** IDS basados en el comportamiento

Explicación

Los detectores de uso indebido se consideran un IDS basado en firmas. Un IDS basado en firmas analiza una base de datos de ataques conocidos y sus respectivos patrones.

Cada ataque basado en la red tiene un patrón único y forma una firma única que puede ser rastreada por el IDS para detectar actividad maliciosa. La base de datos de firmas debe actualizarse periódicamente para realizar un seguimiento de los últimos ataques y sus variaciones. Esta es una desventaja de los IDS basados en firmas. Un patrón de tráfico que no califica como firma válida de un ataque se considera actividad normal y es aceptado por el IDS. Estos tipos de IDS no pueden aprender con el tiempo.

Un IDS basado en el comportamiento funciona supervisando el tráfico de red en tiempo real y se somete a un período de entrenamiento durante el cual se establece el perfil de un usuario normal y el patrón de tráfico. Un IDS basado en el comportamiento también se conoce como un IDS basado en anomalías estadísticas. Cualquier anomalía en el patrón de tráfico depende de la desviación estadística del perfil existente y se notifica. La principal ventaja del IDS basado en el comportamiento es su capacidad para detectar ataques desconocidos que no se han notificado. En este IDS, la base de datos de firmas no necesita ser actualizada constantemente. El principal inconveniente es el número de falsas alarmas generadas por un IDS basado en el comportamiento. Estos tipos de IDS pueden aprender con el tiempo.

Los IDS basados en tiempo y de control de acceso no son tipos válidos de IDS. Los IDS basados en host y los IDS basados en red se dividen en dos categorías: basados en firmas y basados en comportamientos. Un IDS se ejecuta en tiempo real y puede monitorear cada evento o solo ciertos eventos, dependiendo de su configuración.

Objetivo:
Operaciones de seguridad

Subobsecución:
Llevar a cabo actividades de registro y vigilancia

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 4: Comunicación y Seguridad de red, IDS

Pregunta #125 de 163

Id. de pregunta: 1105513

Administrar una pequeña red corporativa. El viernes por la noche, después del cierre de los negocios, realizó una copia de seguridad completa del disco duro de uno de los servidores de la compañía. El lunes por la noche, realizó una copia de seguridad diferencial del disco duro del mismo servidor y los martes, miércoles y jueves por la noche realizó copias de seguridad incrementales del disco duro del servidor.

¿Qué archivos se registran en la copia de seguridad que realizó el jueves?

- ✗ **A)** Todos los archivos del disco duro que se cambiaron o crearon desde la copia de seguridad incremental del martes
- ✗ **B)** Todos los archivos del disco duro
- ✗ **C)** Todos los archivos del disco duro que se cambiaron o crearon desde la copia de seguridad diferencial del lunes
- ✓ **D)** Todos los archivos del disco duro que se cambiaron o crearon desde la copia de seguridad incremental del miércoles

Explicación

Realizó una copia de seguridad el miércoles, por lo que la copia de seguridad incremental que realizó el jueves realizó una copia de seguridad de todos los archivos en el disco duro que se cambiaron o crearon desde la copia de seguridad del miércoles. El jueves, realizó una copia de seguridad incremental del disco duro. Una copia de seguridad incremental realiza una copia de seguridad de los archivos que se han creado o cambiado desde la copia de seguridad completa o incremental inmediatamente anterior. Con una estrategia de copia de seguridad completa/copia de seguridad incremental, la restauración requiere que la copia de seguridad completa y todas las copias de seguridad incrementales desde la última copia de seguridad completa se restauren en orden.

Una copia de seguridad diferencial realiza una copia de seguridad de los archivos que se han creado o cambiado desde la última copia de seguridad completa. En una estrategia de copia de seguridad completa/copia de seguridad diferencial, es necesario restaurar la copia de seguridad completa y SOLO la copia de seguridad diferencial reciente del movimiento.

Objetivo:
Operaciones de seguridad

Subobsecución:
Implementar estrategias de recuperación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, tipos de copia de seguridad de datos y esquemas

---

Pregunta #126 de 163

Id. de pregunta: 1111802

Haga coincidir las descripciones de la derecha con los ataques de ingeniería social de la izquierda.

{UCMS id=5678026064920576 type=Activity}

Explicación

Los ataques de ingeniería social deben coincidir con las descripciones de la siguiente manera:

- Surf de hombro - observar a alguien cuando ingresa datos confidenciales
- Tailgating - siguiendo a alguien a través de una puerta que acaba de abrir
- Vishing - un tipo especial de phishing que utiliza VoIP
- Caza de ballenas: un tipo especial de phishing que se dirige a un solo usuario avanzado

Objetivo:
Operaciones de seguridad

Subobsecución:
Abordar las preocupaciones de seguridad y protección del personal

Referencias:

Cissp Cert Guide (3ª Edición), Glosario

Pregunta #127 de 163

Id. de pregunta: 1114006

Durante un desastre natural reciente, se destruyó la ubicación principal de su organización. Para poner en línea el sitio alternativo, primero ha restaurado los sistemas más críticos. Ahora se ha completado un nuevo sitio primario y debe asegurarse de que el sitio se pone en línea de forma ordenada. ¿Qué debes hacer primero?

- ✗ **A)** Restaure todas las funciones interdependientes en el nuevo sitio primario.
- ✗ **B)** Restaure todas las funciones independientes en el nuevo sitio primario.
- ✓ **C)** Restaure las funciones menos críticas en el nuevo sitio primario.
- ✗ **D)** Restaure las funciones más críticas en el nuevo sitio primario.

Explicación

Al realizar la fase de reconstitución de la recuperación, primero debe restaurar las funciones menos críticas en el nuevo sitio primario. Entonces, si hay problemas con el nuevo sitio, las operaciones críticas de la empresa no se ven afectadas negativamente. Si las funciones menos críticas funcionan correctamente, entonces usted sube la escalera a las siguientes funciones menos críticas. Las últimas funciones que se deben mover al nuevo sitio primario son las funciones más críticas.

Mientras que las funciones más críticas deben restaurarse primero en el sitio alternativo, las funciones más críticas deben moverse LAST en el sitio primario original o nuevo.

Objetivo:
Operaciones de seguridad

Subobsecución:
Implementar procesos de recuperación ante desastres (DR)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y gestión de riesgos, recuperación ante desastres y el plan de recuperación ante desastres (DRP)

Pregunta #128 de 163

Id. de pregunta: 1105436

La red de su empresa ha sido violada. Durante la violación, el atacante elimina los datos incriminatorios de los registros de auditoría de su empresa para evitar el enjuiciamiento. ¿Cómo se llama este proceso?

- ✗ **A)** limpieza
- ✗ **B)** claro
- ✗ **C)** Eliminar

✓ **D)** Fregar

Explicación

El barrido es el proceso de eliminar datos incriminatorios de los registros de auditoría.

Al borrar los registros de auditoría, se quitan todos los datos de los registros. Al eliminar los registros de auditoría, se quitan los propios registros.

No hay ningún proceso de limpieza en lo que se refiere a los registros de auditoría.

Debe limitar el acceso a los registros de auditoría. Los usuarios, incluidos los administradores de seguridad, deben tener acceso de solo lectura a los registros del sistema. Los controles de seguridad deben estar en su lugar para asegurarse de que los registros del sistema se copian correctamente antes de eliminarlos de su sistema. Solo personas de confianza

Objetivo:
Operaciones de seguridad

Subobsecución:
Llevar a cabo actividades de registro y vigilancia

Referencias:

CISSP Cert Guide (3rd Edition), Chapter 5 Identity and Access Management Auditing and Reporting

---

Pregunta #129 de 163

Id. de pregunta: 1192970

¿Qué tipo de incidente NO se aborda generalmente en un plan de contingencia?

✗ **A)** un error de conexión T1
✓ **B)** un huracán
✗ **C)** un corte de energía
✗ **D)** un bloqueo del servidor

Explicación

Por lo general, un huracán no se aborda en un plan de contingencia. Todos los desastres naturales forman parte del plan de continuidad de las actividades, no del plan de contingencia.

El plan de contingencia aborda cómo lidiar con pequeños incidentes, como cortes de energía, fallas de conexión, bloqueos del servidor y daños en el software.

Objetivo:
Operaciones de seguridad

Subobsecución:
Implementar procesos de recuperación ante desastres (DR)

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, Plan de Contingencia

---

Pregunta #130 de 163

Id. de pregunta: 1111801

Su organización le ha pedido que vuelva a evaluar el plan de seguridad de la organización para ver si aborda completamente la prevención de delitos e interrupciones a través de la disuasión. ¿Qué mecanismo de seguridad cubre esta cuestión?

- ✓ **A)** Cercas
- ✗ **B)** detectores de humo
- ✗ **C)** notificación de aplicación de la ley
- ✗ **D)** evaluación del nivel de daño

Explicación

Las vallas abordan la prevención de la delincuencia y las perturbaciones mediante la disuasión. Otros mecanismos que encajan en esta categoría incluyen guardias de seguridad, señales de advertencia y cerraduras.

La evaluación del nivel de daños es parte de la evaluación de incidentes. No tiene nada que ver con la disuasión.

La notificación de aplicación de la ley cubre los procedimientos de respuesta. Los procedimientos de respuesta también incluyen la extinción de incendios y la consulta de seguridad externa.

Los detectores de humo cubren la detección de interrupciones. La detección de delitos o interrupciones también incluye detectores de movimiento y circuitos cerrados de televisión (CCTV).

El plan de seguridad de una organización debe abordar las siguientes áreas:

- Prevención del crimen y la interrupción a través de la disuasión - incluye cercas, guardias de seguridad y cerraduras
- Reducción de daños mediante mecanismos de retardo: incluye capas de defensa que utilizan cerraduras, personal de seguridad y barreras
- Detección de delitos o interrupciones: incluye detectores de humo, detectores de movimiento, sistemas de detección de intrusiones (IDS) y CCTV

- Evaluación de incidentes : incluye la respuesta de los guardias de seguridad a los incidentes y la evaluación del nivel de daños.
- Procedimientos de respuesta : incluyen la supresión de incendios, los procesos de respuesta a emergencias, la notificación de las fuerzas del orden y la consulta externa de seguridad.

Objetivo:
Operaciones de seguridad

Subobjetiva:
Implementar y administrar la seguridad física

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 3: Arquitectura e Ingeniería de Seguridad, CPTED

Pregunta #131 de 163

Id. de pregunta: 1114782

Debido al valor de los datos de su empresa, su empresa le ha pedido que garantice la disponibilidad de los datos. Desea implementar las técnicas que pueden ayudar a garantizar la disponibilidad de los datos. ¿Qué mecanismo(s) debe(n) implementar?

a. Técnicas de auditoría

b. Técnicas de recuperación de datos

c. Técnicas de autenticación

d. Técnicas de tolerancia a fallos

e. técnicas de control de acceso

✗ **A)** Sólo las opciones A y C
✗ **B)** opción b
✗ **C)** opción e
✗ **D)** opción A
✗ **E)** Opción d
✓ **F)** Opciones B y D Sólo
✗ **G)** opción c

Explicación

Debe implementar técnicas de recuperación de datos y tolerancia a errores para garantizar la disponibilidad de los datos. Las técnicas de tolerancia a errores funcionan para garantizar que los datos estén disponibles en caso de error de hardware. Las técnicas de recuperación de datos funcionan para garantizar que una copia alternativa de los datos esté disponible en caso de error del sistema.

Ninguna de las otras técnicas funciona para garantizar la disponibilidad de los datos.

Las técnicas de auditoría y autenticación funcionan para garantizar la responsabilidad del usuario y la integridad de los datos. Las técnicas de control de acceso funcionan para garantizar la confidencialidad e integridad de los datos.

Objetivo:
Operaciones de seguridad

Subobsecución:
Implementar estrategias de recuperación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y gestión de riesgos, tolerancia a fallos

---

Pregunta #132 de 163

Id. de pregunta: 1111772

El gobierno de Estados Unidos está investigando un crimen. Se han puesto en contacto con usted en relación con la evidencia que se encuentra en los servidores de su organización. ¿Qué método NO es utilizado por la policía federal para obtener información?

- ✗ **A)** interrogar al sospechoso para que revele la información
- ✗ **B)** obtener una orden judicial
- ✗ **C)** obtener una orden de registro
- ✓ **D)** siguientes procedimientos subrayados en la Quinta Enmienda

Explicación

La Quinta Enmienda no es utilizada por la policía federal para obtener información sobre un incidente.

La policía federal no puede tomar acciones legales contra un sospechoso a menos que se hayan reunido pruebas sólidas contra el sospechoso y el caso se presente en el tribunal de justicia. El caso es presentado por expertos legales en nombre del organismo de investigación.

La policía federal obtiene información sobre un ataque mediante el uso de algunos de los siguientes métodos:

- obtener una orden judicial contra el sospechoso

- obtener una orden de registro
- entrevistar e interrogar al sospechoso
- seguir los procedimientos de conformidad con los derechos de la Cuarta Enmienda de los ciudadanos estadounidenses, a menos que haya exigencias

Se puede emitir una orden de registro si existe la probabilidad de que se haya cometido un delito si se espera que haya pruebas del delito o si hay una razón probable para entrar en la casa o negocio de alguien.

La policía federal examina los registros de auditoría y los registros del sistema, entrevista a testigos y evalúa los daños incurridos como resultado del ataque. Se emite una orden de registro para un lugar específico si hay una razón probable para el registro, además de la anticipación documentada de la evidencia. Los ciudadanos estadounidenses están protegidos por los derechos de la Cuarta Enmienda. Por lo tanto, la agencia de aplicación de la ley debe tener una razón probable para solicitar una orden de registro de la corte.

Durante la investigación de un delito informático, las pistas de auditoría pueden ser útiles. Para garantizar que el registro de auditoría se pueda utilizar como prueba, se deben seguir ciertos procedimientos, entre ellos:

- La información de la pista de auditoría debe utilizarse durante el curso normal de los negocios.
- Debe haber una directiva de seguridad organizativa válida en vigor y en uso que defina el uso de la información de auditoría.
- Deben existir mecanismos para proteger la integridad de la información de la pista de auditoría.

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender los requisitos para los tipos de investigación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, vigilancia, registro e incautación

---

Pregunta #133 de 163

Id. de pregunta: 1105518

Su organización ha creado un plan de recuperación ante desastres exhaustivo. ¿Cuándo debe aplicarse?

✗ **A)** Después de que todos los sistemas vuelvan a estar en línea
✗ **B)** Cuando la empresa está en modo de funcionamiento normal
✗ **C)** Una vez que los sistemas críticos vuelven a estar en línea
✓ **D)** Cuando la empresa está en modo de emergencia

Explicación

Un plan de recuperación ante desastres se implementa cuando la empresa está en modo de emergencia. Un plan de recuperación ante desastres se ocupa de cualquier desastre que se produzca y proporciona una forma de volver a poner en línea todos los sistemas críticos. Un desastre se considera oficialmente terminado cuando todos los elementos del negocio han vuelto a funcionar normalmente en el sitio original. La prioridad número uno de la respuesta a los desastres es la seguridad del personal. La organización tiene la responsabilidad de continuar con los salarios u otros fondos para los empleados y/o familias afectadas por el desastre.

Un plan de copia de seguridad se implementa cuando la empresa está en modo de funcionamiento normal. Sin un plan de copia de seguridad adecuado, un plan de recuperación ante desastres es casi imposible.

Un plan de continuidad del negocio incluye el plan de recuperación ante desastres. El plan de continuidad del negocio tiene un enfoque más amplio que el plan de recuperación ante desastres. Se centra en cómo mantenerse en el negocio hasta que la operación vuelva a la normalidad.

Objetivo:
Operaciones de seguridad

Subobsecución:
Implementar procesos de recuperación ante desastres (DR)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y gestión de riesgos, recuperación ante desastres y el plan de recuperación ante desastres (DRP)

Pregunta #134 de 163

Id. de pregunta: 1114002

Su organización ha respondido a un incidente de seguridad. La brecha ha sido contenida, y todos los sistemas han sido recuperados. ¿Qué debe hacer por último como parte de la respuesta al incidente?

- ✓ **A)** revisión post mortem
- ✗ **B)** análisis
- ✗ **C)** clasificación
- ✗ **D)** investigación

Explicación

Una revisión post mortem debe completarse en último lugar como parte de la respuesta al incidente. La revisión post mortem debe realizarse dentro de la primera semana de completar la investigación de la intrusión.

El triaje es parte del primer paso en una respuesta a un incidente. Durante este paso, el equipo de respuesta a incidentes examina el incidente para ver qué se vio afectado y establece prioridades.

La investigación se lleva a cabo después del triaje. Se trataba de la recopilación de datos pertinentes. Después de la etapa de investigación, el equipo de respuesta a incidentes es responsable de la etapa de contención.

Una vez contenido el incidente, la siguiente etapa es el análisis, donde se determina la causa raíz del problema.

Objetivo:
Operaciones de seguridad

Subobsecución: Llevar
a cabo la gestión de incidentes

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, gestión de respuesta a incidentes

---

Pregunta #135 de 163

Id. de pregunta: 1113998

¿Qué cuaderno es el más preferido durante el curso de la investigación en el mantenimiento de registros legales?

- ✓ **A)** bloc de notas enlazado
- ✗ **B)** Bloc de notas claro
- ✗ **C)** bloc de notas etiquetado
- ✗ **D)** cuaderno espiral

Explicación

Al recopilar y analizar pruebas en el mantenimiento de registros legales, el equipo de respuesta debe registrar los hallazgos en un cuaderno encuadernado en lugar de en un cuaderno en espiral.

Mientras sigue la cadena de custodia, el equipo de respuesta debe estar equipado con un cuaderno encuadernado, una cámara, herramientas forenses, contenedores y etiquetas de identificación de evidencia. Los blocs de notas enlazados son útiles porque la eliminación de páginas se nota fácilmente.

Los cuadernos espirales no deben usarse porque no hay una forma clara de notar si se han eliminado las páginas. Los cuadernos etiquetados y los cuadernos claros son categorías no válidas de cuadernos utilizados por el investigador durante el curso de la recopilación y el análisis de pruebas.

Es importante tener en cuenta que el cuaderno no se puede utilizar como evidencia en la corte. Un cuaderno como parte del mantenimiento de registros legales solo puede ser utilizado por el investigador para refrescar la memoria de

esa persona durante las audiencias y mientras presenta los hechos y las pruebas al tribunal.

Durante el curso de la investigación y mientras se sigue la cadena de custodia, la escena del delito informático debe ser fotografiada junto con el etiquetado adecuado y las etiquetas adjuntas a la evidencia. El contenido de la memoria del equipo debe volcarse y el sistema debe apagarse. Una imagen de bits del disco duro debe estar preparada para ser utilizada para la investigación.

Para que las pruebas sean admisibles en un tribunal de justicia, deben ser pertinentes, legalmente permisibles, confiables, debidamente identificadas y debidamente preservadas. La fiabilidad de las pruebas significa que las pruebas no han sido manipuladas ni modificadas.

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender los requisitos para los tipos de investigación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, preservar y recopilar evidencia

---

Pregunta #136 de 163

Id. de pregunta: 1105531

Su organización está investigando instalaciones informáticas alternativas para asegurarse de que la organización puede funcionar si se destruye la instalación principal. ¿Qué instalación fuera del sitio es la más costosa de implementar?

- ✗ **A)** sitio cálido
- ✓ **B)** sitio caliente
- ✗ **C)** sitio frío
- ✗ **D)** mecanismo de ayuda mutua

Explicación

Un sitio caliente es la instalación fuera del sitio más costosa de implementar. Un sitio caliente es una instalación de copia de seguridad que es propiedad de otra empresa y se puede llevar a la línea con relativa facilidad. La empresa que necesita los servicios de copia de seguridad paga una tarifa al propietario. El propietario es responsable de la gestión del sitio caliente. Si se produce un desastre en el sitio primario, el sitio caliente se pone en línea rápida y fácilmente.

Los sitios calientes y los sitios redundantes suelen ser los más costosos de implementar. Los sitios cálidos son menos costosos que los sitios calientes, pero más caros que los sitios fríos. Los sitios fríos son los menos costosos de implementar. Todas estas entidades a veces se conocen como reemplazos de almacenamiento fuera del sitio. Las instalaciones fuera del sitio deben estar lo suficientemente lejos de la instalación original para que el mismo desastre no afecte a ambos lugares.

Un sitio caliente es una instalación de copia de seguridad que es propiedad de otra empresa y está parcialmente configurada, normalmente excluyendo los servidores. Si se produce un desastre en el sitio primario, la empresa que necesita el servicio llevaría el hardware y el software al sitio para su instalación.

Un sitio frío es una instalación de respaldo que es propiedad de otra compañía y solo incluye un alquiler de habitación básico, como electricidad, aire acondicionado, plomería, etc. Si se produce un desastre en el sitio primario, el sitio frío tendría que configurarse por completo, a veces tardando semanas en configurarse.

Un sitio de ayuda mutua es un sitio establecido en una empresa con la que su empresa tiene un acuerdo recíproco. Un acuerdo recíproco es aquel en el que las partes acuerdan acudir en ayuda de la otra en caso de catástrofe proporcionando una instalación alternativa. Esta suele ser la más barata de las opciones fuera del sitio, pero por lo general no funcionan bien. Los acuerdos recíprocos son difíciles de hacer cumplir aunque se basen en contratos y acuerdos. Los acuerdos recíprocos no deben utilizarse en situaciones en las que el período de continuidad del negocio sea bajo, lo que significa que la recuperación del sitio debe producirse rápidamente.

Un sitio redundante es una instalación de copia de seguridad que es propiedad de la empresa y se puede llevar a la línea con relativa facilidad. También es gestionado por la empresa. En la mayoría de los casos, un sitio redundante está caliente, lo que significa que está listo inmediatamente para la producción. Si se produce un desastre en el sitio primario, el sitio redundante se pone en línea fácilmente.

Un sitio redundante generalmente se mantiene dentro de la empresa y no requiere ningún contrato con un proveedor fuera del sitio. Otros sitios que generalmente se mantienen dentro de la empresa incluyen sitios móviles y múltiples centros de procesamiento. Los sitios calientes, cálidos y fríos generalmente son mantenidos por un proveedor fuera del sitio y requieren un contrato de proveedor.

Tanto el sitio caliente como el sitio redundante son los más fáciles de probar porque ambos contienen todos los equipos informáticos y de telecomunicaciones alternativos necesarios en un desastre. Por lo general, probar cualquiera de estos entornos es tan simple como cambiar a ellos después de asegurarse de que contienen las versiones más recientes de los datos.

Un sitio caliente es más difícil de probar que un sitio caliente o un sitio redundante, pero más fácil de probar que un sitio frío. Sólo contiene el equipo de telecomunicaciones. Por lo tanto, para probarlo correctamente, sería necesario instalar y configurar equipos informáticos alternativos.

Un sitio frío es el más difícil de probar. Solo incluye una habitación básica con pisos elevados, cableado eléctrico, aire acondicionado, etc. Para probarlo correctamente, sería necesario instalar y configurar equipos alternativos de telecomunicaciones e informática.

Objetivo:
Operaciones de seguridad

Subobsecución:
Probar planes de recuperación ante desastres (DRP)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, Hot Site

---

Pregunta #137 de 163

Id. de pregunta: 1192968

¿Cuándo debe instalar una revisión de software en un servidor de producción?

- ✗ **A)** Cuando la revisión está en formato beta
- ✓ **B)** Una vez probada la revisión
- ✗ **C)** antes de que se haya probado la revisión
- ✗ **D)** inmediatamente después del lanzamiento del parche

Explicación

Se debe instalar una revisión en un servidor después de que la revisión haya sido probada en un servidor que no sea de producción y por la comunidad informática. Un parche de seguridad es una actualización importante y crucial para un sistema operativo o producto para el que está destinado y consiste en una colección de parches publicados hasta la fecha desde que se envió el sistema operativo o el producto. Una revisión de seguridad es obligatoria para todos los usuarios, corrige una nueva vulnerabilidad y debe implementarse lo antes posible. Los parches de seguridad suelen ser de pequeño tamaño.

Un parche no debe instalarse inmediatamente después de su lanzamiento o cuando está en formato beta porque un parche que no se ha probado exhaustivamente puede contener errores que podrían ser perjudiciales para el funcionamiento del servidor. Normalmente, una revisión no debe implementarse antes de que se haya probado en un servidor de prueba; las revisiones no deben probarse en servidores de producción.

Una hot fix es una corrección de software no completamente probada que aborda un problema específico que experimentan ciertos clientes.

Objetivo:
Operaciones de seguridad

Subobsecución:
Implementar y apoyar la gestión de parches y vulnerabilidades

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, gestión de parches y vulnerabilidades

---

Pregunta #138 de 163

Id. de pregunta: 1111796

Se le ha pedido que trabaje con un equipo para diseñar el plan de continuidad del negocio de su empresa. El equipo ha definido el alcance del plan de continuidad del negocio. ¿Cuál es el siguiente paso?

✗ **A)** Identificar funciones críticas.

✗ **B)** Identificar las dependencias entre las áreas de negocio y las funciones críticas.

✓ **C)** Identificar las áreas de negocio clave.

✗ **D)** Determine el tiempo de inactividad aceptable.

Explicación

El siguiente paso en el diseño del plan de continuidad del negocio es identificar las áreas de negocio clave.

Los pasos para diseñar el plan de continuidad del negocio son los siguientes:

- Identifique el alcance del plan.
- Identificar áreas de negocio clave.
- Identificar funciones críticas.
- Identificar las dependencias entre las áreas de negocio y las funciones críticas.
- Determine el tiempo de inactividad aceptable para cada función crítica.
- Cree un plan para mantener las operaciones.

Objetivo:
Operaciones de seguridad

Subobsecución:
Implementar procesos de recuperación ante desastres (DR)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Planificación de continuidad y el Plan de Continuidad del Negocio (BCP)

Pregunta #139 de 163

Id. de pregunta: 1105469

Como administrador de seguridad de una organización, debe evitar conflictos de intereses al asignar personal para completar determinadas tareas de seguridad. ¿Qué principio de seguridad de operaciones está implementando?

- ✓ **A)** separación de funciones
- ✗ **B)** rotación de trabajos
- ✗ **C)** Debida diligencia
- ✗ **D)** atención debida

Explicación

Cuando se evitan conflictos de intereses al asignación de personal para completar determinadas tareas de seguridad, se está implementando la separación de funciones. La separación de funciones es una medida preventiva. Para cometer un acto ilegal, la colusión debe ocurrir entre el personal.

La diligencia debida se produce cuando se evalúa la información para identificar vulnerabilidades, amenazas y problemas relacionados con el riesgo.

El debido cuidado se produce cuando una organización ha tomado las medidas necesarias para proteger la organización, sus recursos y personal.

La rotación de trabajos se produce cuando más de una persona completa las tareas de un solo puesto dentro de la organización.

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender y aplicar conceptos fundamentales de operaciones de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, separación de funciones

---

Pregunta #140 de 163

Id. de pregunta: 1105404

¿Qué término de delito se utiliza para indicar cómo un delincuente cometió un delito?

- ✓ **A)** medio
- ✗ **B)** MAMÁ
- ✗ **C)** motivo
- ✗ **D)** oportunidad

Explicación

Los medios se utilizan para indicar cómo un criminal cometió el delito.

Motivo es el término utilizado para indicar por qué se comete un delito. La oportunidad se utiliza para indicar cuándo y dónde ocurrió un delito.

El motivo, la oportunidad y los medios (MOM) son los tres principios del crimen que se investigan cuando ocurre un crimen.

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender y apoyar las investigaciones

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, MOM

Pregunta #141 de 163

Id. de pregunta: 1105550

¿Qué es una barrera física que actúa como la primera línea de defensa contra un intruso?

- ✗ **A)** un bloqueo
- ✗ **B)** un mantrap
- ✓ **C)** una valla
- ✗ **D)** un torniquete

Explicación

La esgrima actúa como la primera línea de defensa contra los intrusos ocasionales y los posibles intrusos, pero la esgrima debe complementarse con otros controles de seguridad física, como guardias y perros, para mantener la seguridad de la instalación. Una altura de la cerca de 6 a 7 pies se considera ideal para evitar que los intrusos trepar por encima de la cerca. Además de ser una barrera para los intrusos, la valla también puede controlar las multitudes. Una altura de cerca de 3 a 4 pies actúa como una protección contra los intrusos ocasionales. Para áreas críticas, la cerca debe tener al menos 8 pies de altura con tres hebras de alambre de púas.

Los bloqueos son un ejemplo de controles de seguridad físicos. Una organización puede utilizar bloqueos para evitar el acceso no autorizado o para inducir un retraso en el proceso de una infracción de seguridad. Las cerraduras deben

usarse en combinación con otros controles de seguridad para proteger la infraestructura de la instalación y sus recursos críticos. Las cerraduras generalmente no sirven como la primera línea de defensa contra los intrusos.

Los torniquetes y los mantraps no sirven como primera línea de defensa contra un intruso. Un torniquete es un tipo de puerta que permite el movimiento en una sola dirección a la vez. Un mantrap se refiere a un conjunto de puertas dobles generalmente monitoreadas por un guardia de seguridad.

Objetivo:
Operaciones de seguridad

Subobjetiva:
Implementar y administrar la seguridad física

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de Seguridad, Vallas

---

Pregunta #142 de 163

Id. de pregunta: 1114770

Recientemente, un empleado utilizó el equipo que le asignó su organización para llevar a cabo un ataque contra la organización. Se le ha pedido que recopile todas las pruebas relacionadas con el sistema. Debe recopilar la evidencia utilizando el orden de volatilidad para preservar la evidencia.

Mueva los tipos de datos de la columna izquierda a la columna derecha y colótelos en el orden correcto de volatilidad, comenzando con el más volátil en la parte superior. (Se utilizarán todos los componentes).

{UCMS id=5674327829643264 type=Activity}

Explicación

Utilizando el orden de volatilidad para preservar la evidencia, la evidencia debe preservarse en el siguiente orden:

Memoria (MÁS volátil)

Procesos de red

Procesos del sistema

Disco duro

Cintas de backup

DVD (MENOS volátil)

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender y apoyar las investigaciones

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 7: Operaciones de Seguridad, Investigaciones

---

Pregunta #143 de 163

Id. de pregunta: 1111790

Hacer coincidir las descripciones de la izquierda con el tipo de malware a la derecha que mejor coincide con la descripción.

{UCMS id=5754744247156736 type=Activity}

Explicación

Los tipos de malware deben coincidir con las descripciones de la siguiente manera:

- Adware - una aplicación de software que muestra anuncios mientras se ejecuta la aplicación
- Botnet - un ordenador que es hackeado cuando un programa malicioso está instalado en él y se activa de forma remota
- Rootkit - una colección de programas que concede a un hacker acceso administrativo a un ordenador o red
- Gusano - un programa que se propaga a través de conexiones de red

Objetivo:
Operaciones de seguridad

Subobsecución:
Operar y mantener medidas detectivescas y preventivas

Referencias:

Cissp Cert Guide (3ª Edición), Glosario

Pregunta #144 de 163

Id. de pregunta: 1114007

¿Qué plan está escrito para intentar evitar que un desastre afecte a la organización y/o para disminuir el impacto de un desastre?

- ✗ **A)** proceso de gestión de incidentes
- ✓ **B)** plan de continuidad del negocio
- ✗ **C)** análisis de impacto en el negocio
- ✗ **D)** plan de recuperación ante desastres

Explicación

El plan de continuidad del negocio está escrito para intentar evitar que un desastre afecte a la organización o para disminuir el impacto de un desastre en la organización.

Se escribe un plan de recuperación ante desastres para recuperarse cuando se produce un desastre. El análisis de impacto en el negocio está escrito para determinar el impacto de cada desastre que su organización considera que debe tenerse en cuenta. El proceso de administración de incidentes está diseñado para controlar cualquier incidente, como infracciones de seguridad.

Objetivo:
Operaciones de seguridad

Subobsecución:
Implementar procesos de recuperación ante desastres (DR)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Planificación de continuidad y el Plan de Continuidad del Negocio (BCP)

Pregunta #145 de 163

Id. de pregunta: 1192963

¿Qué método de restablecimiento de la contraseña del BIOS requiere acceso físico al equipo?

- ✓ **A)** restablecer el contenido de CMOS a través de hardware
- ✗ **B)** descifrar la contraseña del BIOS
- ✗ **C)** restablecer el contenido de CMOS a través de software
- ✗ **D)** uso de una contraseña de BIOS de puerta trasera

Explicación

Restablecer el contenido de CMOS a través de hardware requiere acceso físico al equipo. Para restablecer el contenido de CMOS a través de hardware, tendría que abrir la caja de la computadora y activar los puentes que restablecen el contenido de CMOS, o quitar la batería CMOS por completo.

Los otros métodos enumerados no requieren acceso físico al equipo. Puede restablecer el contenido de CMOS a través de software de forma remota. Otros métodos remotos incluyen descifrar la contraseña del BIOS y usar una contraseña del BIOS de puerta trasera.

Las puertas traseras son aquellas aplicaciones que los proveedores crean para garantizar que puedan acceder a sus dispositivos. Después de instalar nuevos dispositivos o sistemas operativos, debe asegurarse de que todas las puertas traseras y contraseñas predeterminadas estén deshabilitadas o restablecidas. A menudo, los hackers primero intentan usar tales puertas traseras y contraseñas predeterminadas para acceder a nuevos dispositivos.

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender y aplicar conceptos fundamentales de operaciones de seguridad

Referencias:

¿Por qué molestarse en la seguridad del BIOS?, HYPERLINK "https://www.sans.org/reading-room/whitepapers/threats/bother-about-bios-security-108" \t "sean" http://www.sans.org/reading_room/whitepapers/threats/108.php

---

Pregunta #146 de 163

Id. de pregunta: 1105515

¿Qué solución de copia de seguridad electrónica realiza copias de seguridad de los datos en tiempo real pero transmite los datos a una instalación fuera del sitio en lotes?

- ✓ **A)** bóveda electrónica
- ✗ **B)** sombreado de disco
- ✗ **C)** registro en diario remoto
- ✗ **D)** administración jerárquica del almacenamiento (HSM)

Explicación

La bóveda electrónica realiza una copia de seguridad de los datos en tiempo real, pero transmite los datos a una instalación fuera del sitio en lotes.

El registro en diario remoto también transmite datos fuera del sitio. Sin embargo, sólo el diario o el registro de transacciones se copia en la instalación fuera del sitio. Esto significa que solo se realiza una copia de seguridad de los cambios en los datos. Con esta solución, los datos perdidos tendrían que ser reconstruidos.

La administración jerárquica del almacenamiento de información (HSM) proporciona una copia de seguridad en línea continua mediante varios dispositivos, incluidas unidades ópticas o de cinta. La ubicación de almacenamiento de datos se basa en la frecuencia con la que se accede a los datos. Los dispositivos más rápidos almacenan datos a los que se accede con más frecuencia; los dispositivos más lentos almacenan datos a los que se accede con menos frecuencia. Un HSM a veces se conoce como una jukebox.

El sombreado de disco también se conoce como duplicación de disco o RAID 1. Esta técnica copia inmediatamente los datos en un segundo disco físico cuando los datos se escriben en el primer disco.

Objetivo:
Operaciones de seguridad

Subobsecución:
Implementar estrategias de recuperación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, copia de seguridad electrónica

---

Pregunta #147 de 163

Id. de pregunta: 1192972

Recientemente, las inundaciones dañaron el edificio que alberga el centro de datos de su empresa. Se le ha pedido a su equipo que determine qué funciones se vieron afectadas por la inundación y qué funciones son más críticas. ¿Qué paso de recuperación ante desastres está realizando?

- ✓ **A)** evaluación de daños
- ✗ **B)** estrategia de recuperación
- ✗ **C)** ensayo
- ✗ **D)** análisis de vulnerabilidades

Explicación

Una evaluación de daños determina las funciones que se vieron afectadas por el desastre y qué funciones son más críticas. Esta evaluación suele ser realizada por un equipo de evaluación de daños utilizando el plan de continuidad del negocio.

La estrategia de recuperación incluye todos los procedimientos y directrices que se deben seguir para restaurar las funciones críticas. Se utiliza cuando las funciones se están restaurando después de que se haya producido la evaluación de daños.

La prueba del plan de recuperación ante desastres garantiza que se puedan restaurar las funciones. No se utiliza cuando se produce un desastre real. El objetivo principal de probar una instalación alternativa es garantizar la compatibilidad continua de las instalaciones alternativas.

Un análisis de vulnerabilidades identifica las vulnerabilidades de su empresa. Forma parte del plan de continuidad del negocio, no del plan de recuperación ante desastres.

Algunos de los elementos principales del plan de recuperación ante desastres incluyen la evaluación de impacto, la estrategia de recuperación y las pruebas. La implementación de un plan de recuperación ante desastres debe garantizar la continuidad del negocio, proteger los datos críticos y minimizar el impacto del desastre.

La comunicación durante un desastre es vital, tanto con los empleados como con el público. Por lo general, alguien del comité de continuidad del negocio actúa como portavoz de la empresa durante el período de recuperación ante desastres. Un plan de recuperación ante desastres debe incluir un modelo de comunicación. Este modelo detallará cómo debe producirse la comunicación en el manual del plan, incluyendo cómo se emiten las advertencias y declaraciones y cómo sobrevivirá la empresa.

Siempre es preferible que las malas noticias sean comunicadas por la empresa y no por los medios de comunicación. Sin embargo, es importante que la persona que comunica las noticias sea consciente de todas las ramificaciones legales y económicas de la información que se divulga. Por esta razón, el portavoz suele ser alguien del departamento de relaciones públicas o legal.

Un desastre se considera oficialmente terminado cuando todos los elementos del negocio han vuelto a funcionar normalmente en el sitio original. La organización tiene la responsabilidad de continuar con los salarios u otros fondos para los empleados y/o familias afectadas por el desastre.

Objetivo:
Operaciones de seguridad

Subobsecución:
Participar en la planificación y los ejercicios de continuidad del negocio (BC)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, equipo de evaluación de daños

---

Pregunta #148 de 163

Id. de pregunta: 1105435

¿Qué herramienta es un sistema de detección de intrusiones (IDS)?

- ✗ **A)** Nessus
- ✗ **B)** Tripwire

✓ **C)** Resoplar

✗ **D)** Etéreo

Explicación

Snort es un sistema de detección de intrusiones (IDS).

Nessus es una herramienta de evaluación de vulnerabilidades. Tripwire es un comprobador de integridad de archivos. Ethereal es un analizador de protocolos de red.

Objetivo:
Operaciones de seguridad

Subobsecución:
Llevar a cabo actividades de registro y vigilancia

Referencias:

Las 75 mejores herramientas de seguridad, http://sectools.org/tools2003.html

---

Pregunta #149 de 163

Id. de pregunta: 1114773

Ha decidido utilizar un sistema de detección de intrusiones basado en host (HIDS) para proporcionar mayor seguridad en la red de su empresa. ¿Qué fuentes de información NO son utilizadas por este sistema para analizar un intento de intrusión?

a. Registros del sistema

b. Paquetes de red

c. Alarmas del sistema operativo

d. Pistas de auditoría del sistema operativo

✗ **A)** Opciones A y D

✗ **B)** opción c

✗ **C)** Opción d

✗ **D)** opción A

✓ **E)** Opciones B y C

✗ **F)** opción b

Explicación

Un HIDS no comprueba los paquetes de red ni las alarmas del sistema operativo para analizar un intento de intrusión. Un sistema de detección de intrusiones (NIDS) basado en red captura paquetes de red reales y los analiza. Los paquetes de red se capturan de los segmentos de red en los que se coloca el NIDS.

Un HIDS utiliza registros generados por el sistema y registros de seguimiento del sistema operativo como fuentes primarias de información para analizar el curso de los eventos. Aunque las pistas de auditoría del sistema operativo se generan en el nivel de kernel del sistema operativo y son detalladas y seguras, los registros del sistema son de menor tamaño y más fáciles de entender. Por ejemplo, un módulo de software IDS basado en aplicaciones, que es un tipo de HIDS, utiliza los archivos de registro de transacciones de la aplicación para analizar cualquier evento anómalo.

La capacidad de registro de auditoría de un HIDS es de naturaleza local y se limita al único host en el que está instalado. Por lo tanto, el HIDS a veces puede no detectar actividad malintencionada debido a limitaciones de registro de auditoría. Un evento en la red también puede pasar desapercibido porque el HIDS no tiene una capacidad de registro centralizado. Para superar esta desventaja, se ha agregado una capacidad centralizada de administración y presentación de informes a algunos HIDS. Un entorno ideal debe tener un NIDS para cada segmento de red y un HIDS para cada estación de trabajo en el segmento de red. El rendimiento de un sistema en el que está instalado un HIDS se ve afectado negativamente porque HIDS utiliza recursos del sistema para la supervisión.

Los sistemas de detección de intrusiones (IDS) se clasifican por su fuente de información: un HIDS obtiene su información de un solo host de grupo de hosts, mientras que un NIDS obtiene información de todo un segmento de red.

Objetivo:
Operaciones de seguridad

Subobsecución:
Llevar a cabo actividades de registro y vigilancia

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 4: Comunicación y Seguridad de red, IDS

Pregunta #150 de 163

Id. de pregunta: 1105474

La administración le ha notificado que el tiempo medio para reparar (MTTR) un disco duro crítico es demasiado alto. Debe abordar este problema con la menor cantidad de gastos. ¿Qué debes hacer?

✓ **A)** Agregue otra unidad de disco duro e implemente la creación de reflejo de disco.

✗ **B)** Agregue dos unidades de disco duro más e implemente la creación de bandas de disco con paridad.

✗ **C)** Reemplace el disco duro por un disco duro más rápido.

✗ **D)** Agregue otra unidad de disco duro e implemente la creación de bandas de disco.

Explicación

Debe agregar otro disco duro e implementar la creación de reflejo de disco. La creación de reflejos de disco copia el contenido escrito en un disco duro con el otro disco duro. Esto reducirá el MTTR para los datos del disco duro.

Reemplazar el disco duro con un disco duro más rápido solo garantizará que los datos se escriban en el disco duro más rápido. No bajará el MTTR.

No debe agregar dos unidades de disco duro más e implementar la creación de bandas de disco con paridad. Si bien esta solución reduciría el MTTR, es más caro que la creación de reflejos de disco.

No debe agregar otro disco duro e implementar la creación de bandas de disco. La creación de bandas de disco no proporciona redundancia de datos. Sólo proporciona un aumento en el rendimiento del disco duro.

Objetivo:
Operaciones de seguridad

Subobjecución:
Aplicar técnicas de protección de recursos

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 7: Operaciones de Seguridad, MTBF y MTTR

Pregunta #151 de 163

Id. de pregunta: 1105396

¿Qué término de delito se utiliza para indicar cuándo y dónde ocurrió un delito?

✗ **A)** medio
✗ **B)** MAMÁ
✗ **C)** motivo
✓ **D)** oportunidad

Explicación

La oportunidad se utiliza para indicar cuándo y dónde ocurrió un delito.

Los medios se utilizan para indicar cómo un criminal cometió el delito. Motivo es el término utilizado para indicar por qué se comete un delito.

El motivo, la oportunidad y los medios (MOM) son los tres principios del crimen que se investigan cuando ocurre un crimen.

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender y apoyar las investigaciones

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, MOM

Pregunta #152 de 163

Id. de pregunta: 1111798

¿Qué NO es un ejemplo de un control operativo?

- ✓ **A)** un plan de continuidad del negocio
- ✗ **B)** una pista de auditoría
- ✗ **C)** administración de la configuración
- ✗ **D)** un control de copia de seguridad

Explanation

A business continuity plan refers to the procedures undertaken for dealing with long-term unavailability of business processes and resources. Business continuity planning differs from disaster recovery. Disaster recovery aims at minimizing the impact of a disaster. Business continuity planning includes the following steps:

- Moving critical systems to another environment during the repair of the original facility
- Performing operations in a constrained mode with lesser resources till the conditions of the primary facility return to normal.
- Dealing with customers, partners, and shareholders through various channels until the original channel is restored.

Operational controls ensure the confidentiality, integrity, and availability of business operations by implementing security as a continuous process.

Audit trails are operational controls and detective controls. Audit trails identify and detect not only unauthorized users but also authorized users who are involved in unauthorized activities and transactions. Audit trails achieve the security objectives defined by the security policy of an organization, and ensure the accountability of users in the organization.

They provide detailed information regarding the computer, the resource usage, and the activities of users. In the event of an intrusion, audit trails can help identify frauds and unauthorized user activity.

Backup controls, software testing, and anti-virus management are other examples of operational software controls.

La gestión de la configuración es un control operativo. La administración de la configuración identifica los controles y los cambios de auditoría realizados en la base informática de confianza (TCB). Los cambios de auditoría incluyen cambios realizados en las configuraciones de hardware, software y firmware a lo largo del ciclo de vida operativo de los activos de infraestructura. La administración de la configuración garantiza que los cambios en la infraestructura se produzcan de forma controlada y sigan un enfoque de procedimiento. La administración de la configuración también garantiza que los cambios futuros en la infraestructura no infrinjan la directiva de seguridad y los objetivos de seguridad de la organización.

Las cuentas de mantenimiento se consideran una amenaza para los controles operativos. Esto se debe a que las cuentas de mantenimiento suelen ser utilizadas por los piratas informáticos para acceder a los dispositivos de red.

Objetivo:
Operaciones de seguridad

Subobsecución:
Participar en la planificación y los ejercicios de continuidad del negocio (BC)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Planificación de continuidad y el Plan de Continuidad del Negocio (BCP)

Pregunta #153 de 163

Id. de pregunta: 1105488

¿Qué afirmación es cierta de un modo de seguridad multinivel?

- ✗ **A)** La clasificación de datos únicos se utiliza en el modo de seguridad multinivel.
- ✓ **B)** El modo de seguridad multinivel implica el uso de etiquetas de confidencialidad.
- ✗ **C)** El modo de seguridad multinivel está representado por el modelo de muro chino.
- ✗ **D)** El modo de seguridad multinivel se basa en pertenencias basadas en roles.

Explicación

El modo de seguridad multinivel, que a veces se denomina modo de seguridad controlado, asigna el uso de etiquetas de sensibilidad a sujetos y objetos para regular el flujo de información. Un sujeto puede acceder a un objeto si la

etiqueta de sensibilidad del sujeto es mayor o igual que la etiqueta de sensibilidad del objeto. Si la etiqueta de sensibilidad del sujeto es inferior a la etiqueta de sensibilidad del objeto, se deniega al sujeto el acceso al objeto.

El modo de seguridad multinivel implementa el control de acceso obligatorio en lugar del control de acceso basado en roles.

El modelo Bell-LaPadula es un ejemplo del modo de seguridad multinivel, no el modelo de la Muralla China. El modelo de Bell-LaPadula fue el primer modelo matemático de una política de seguridad multinivel utilizada para definir los conceptos de estado de seguridad y modo de acceso, y para delinear reglas de acceso. El modelo de muro chino implementa un control de acceso dinámico basado en las acciones anteriores de un usuario. Por ejemplo, si un usuario intenta el acceso no autorizado a un sistema en una sesión, el modelo implementará la directiva de seguridad en función de esa acción del usuario.

Si los usuarios no cuentan con una aprobación formal y autorización de seguridad para acceder a toda la información procesada por el sistema, el modo de seguridad multinivel permite el procesamiento de la información para diferentes niveles de seguridad. El modo de seguridad multinivel administra la clasificación de varias informaciones. Esto es diferente de un modo de seguridad dedicado donde los usuarios tienen la autorización y la aprobación formal para acceder a los datos dentro del sistema. A diferencia del modo de seguridad multinivel, que maneja varias clasificaciones de información, el modo de seguridad dedicado maneja una sola clasificación.

En un sistema de seguridad multinivel (MLS), la bomba es un dispositivo de flujo de información unidireccional. La bomba fue desarrollada en el Laboratorio de Investigación Naval de los Estados Unidos (NRL). Permite el flujo de información en una sola dirección, desde un nivel inferior de clasificación de seguridad o sensibilidad a un nivel superior. Es un enfoque conveniente para la seguridad multinivel, ya que se puede utilizar para armar sistemas con diferentes niveles de seguridad.

Objetivo:
Operaciones de seguridad

Subobsecución:
Operar y mantener medidas detectivescas y preventivas

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 7: Operaciones de seguridad, modo de seguridad multinivel

---

Pregunta #154 de 163

Id. de pregunta: 1105445

Su organización ha decidido implementar un sistema de detección de intrusiones (NIDS) basado en red. ¿Cuál es la principal ventaja de utilizar este tipo de sistema?

✗ **A)** sin contraataque al intruso

✗ **B)** alto rendimiento de las estaciones de trabajo individuales de la red

✗ **C)** capacidad de analizar información cifrada

✓ **D)** bajo mantenimiento

Explicación

La ventaja principal de NIDS es el bajo mantenimiento implicado en analizar el tráfico en la red. Un NIDS es fácil y económico de manejar porque las firmas no se configuran en todos los host en un segmento de red. La configuración suele producirse en un único sistema, en lugar de en varios sistemas. Los sistemas de detección de intrusiones basados en host (HIDS) son difíciles de configurar y supervisar porque el agente de detección de intrusiones debe instalarse en cada estación de trabajo individual de un segmento de red determinado. Los HID están configurados para utilizar los registros de auditoría del sistema operativo y los registros del sistema, mientras que los NIDS examinan realmente los paquetes de red.

Un NIDS puede contraatacar a un intruso después de detectar una intrusión en la red. Un contraataque se lleva a cabo bloqueando la dirección IP del host malicioso a través de listas de acceso o terminando la conexión existente. Un NIDS también puede enviar una alarma a la estación de administración para solicitar medidas correctivas para evitar intrusiones.

Los hosts individuales no necesitan supervisión en tiempo real porque la intrusión se supervisa en el segmento de red en el que se coloca el NIDS y no en estaciones de trabajo individuales.

Un NIDS no es capaz de analizar información cifrada. Por ejemplo, los paquetes que viajan a través de un túnel de red privada virtual (VPN) no se pueden analizar por el NIDS. La falta de esta capacidad es una desventaja principal de un NIDS.

El alto rendimiento de las estaciones de trabajo en una red no depende del NIDS instalado en la red. Factores como la velocidad del procesador, la memoria y el ancho de banda asignado, afectan al rendimiento de las estaciones de trabajo.

El rendimiento de un NIDS puede verse afectado en un entorno de red conmutada porque el NIDS no podrá analizar correctamente todo el tráfico que se produce en la red en la que no reside. Un HIDS no se ve afectado negativamente por una red conmutada porque se ocupa principalmente de supervisar el tráfico en equipos individuales.

Objetivo:
Operaciones de seguridad

Subobsecución:
Llevar a cabo actividades de registro y vigilancia

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 4: Comunicación y Seguridad de red, IDS

Pregunta #155 de 163

Id. de pregunta: 1111794

Se le ha pedido que diseñe el proceso de gestión de cambios de su empresa. ¿Cuál es el primer paso de este proceso?

- ✓ **A)** Solicitar el cambio.
- ✗ **B)** Evaluar el impacto del cambio.
- ✗ **C)** Aprobar el cambio.
- ✗ **D)** Planifique el cambio.

Explicación

El primer paso del proceso de administración de cambios es solicitar el cambio.

Los pasos del proceso de administración de cambios son los siguientes:

- Solicitar el cambio. Esto incluye solicitar el cambio, determinar el propietario del cambio y justificar el cambio.
- Evaluar el impacto del cambio. Esto incluye analizar el cambio para determinar su impacto y el resultado final del cambio.
- Planifique el cambio. Esto incluye documentar todos los pasos necesarios para el cambio.
- Aprobar el cambio. Esto se completa con el tablero de control de cambios (CCB). Se debe completar una aprobación formal o denegación de cualquier cambio solicitado.
- Implemente el cambio. Esto incluye completar todos los pasos que se documentaron en el paso 3.
- Cierre la solicitud de cambio. Esto incluye validar el cambio, notificar al propietario del cambio que se ha completado y documentar el resultado del cambio.

Si no se aprueba un cambio, debe omitir el paso 5.

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender y participar en los procesos de gestión del cambio

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 7: Operaciones de seguridad, procesos de gestión de cambios

---

Pregunta #156 de 163

Id. de pregunta: 1114787

Para mejorar la seguridad, ¿qué mecanismos deben utilizarse con un bloqueo de cifrado?

a. retraso de la puerta

b.key anulación

c. clave maestra

d. Alarma de rehenes

- ✗ **A)** opción b
- ✗ **B)** opción c
- ✗ **C)** Opciones C y D
- ✗ **D)** opción A
- ✗ **E)** Opción d
- ✓ **F)** todas las opciones
- ✗ **G)** opciones A y B

Explicación

Todos los mecanismos enumerados deben utilizarse con un bloqueo de cifrado.

Un retraso de la puerta es una alerta que se activa si la puerta permanece abierta durante demasiado tiempo.

Una invalidación de clave es una combinación que invalida los procedimientos normales. A menudo es utilizado por los supervisores.

Se utiliza una clave maestra para cambiar el código de acceso.

Una alarma de rehén es una combinación en la que una persona entra si se encuentra en una situación de rehén. Esta combinación permite al usuario acceder al área segura mientras alerta a los funcionarios encargados de hacer cumplir la ley y / o guardias de seguridad.

Otra opción que es importante es un escudo de visibilidad para asegurarse de que alguien no puede ver la combinación que se ha clave.

Las copias de seguridad de la batería también son importantes para los bloqueos de cifrado para garantizar que el bloqueo siga funcionando en caso de fallo de alimentación. También debe configurar el bloqueo de cifrado para desbloquear durante un corte de energía para asegurarse de que nadie está atascado dentro de la instalación. Una vez que falla la batería de respaldo, el bloqueo de cifrado se abre automáticamente.

Objetivo:
Operaciones de seguridad

Subobjetiva:
Implementar y administrar la seguridad física

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Cerraduras

---

Pregunta #157 de 163

Id. de pregunta: 1105486

¿Qué fallo del sistema operativo requiere la intervención del administrador del sistema para la restauración del sistema?

- ✓ **A)** inicio en frío del sistema
- ✗ **B)** reinicio de emergencia
- ✗ **C)** recuperación de confianza
- ✗ **D)** reinicio del sistema

Explicación

Un arranque en frío del sistema requiere la intervención del administrador del sistema para la restauración del sistema.

Un inicio en frío del sistema se produce cuando los procedimientos de recuperación no pueden recuperar el sistema de una base informática de confianza (TCB) repentina o de un error de medios. El sistema permanece en un estado incoherente durante un intento del sistema de recuperarse y normalmente requiere la intervención del usuario o administrador del sistema para el proceso de restauración.

Un arranque en frío del sistema se define en la recuperación de confianza como uno de los riesgos para la seguridad del sistema. La recuperación de confianza de los sistemas requiere que durante un error o error esperado un sistema permanezca en un estado seguro recuperándose o apague de manera adecuada.

Un reinicio del sistema se refiere al arranque del sistema después de que se apaga de manera controlada en respuesta a un error de TCB. Un reinicio del sistema puede ocurrir para liberar los recursos del sistema para realizar las actividades del sistema.

Un reinicio del sistema de emergencia se produce en respuesta a un error del sistema de forma no controlada. Puede deberse a TCB, a un error de medios o a la realización de una actividad insegura, como un proceso con menos privilegios que intenta tener acceso a segmentos de memoria restringidos.

Objetivo:
Operaciones de seguridad

Subobsecución:
Operar y mantener medidas detectivescas y preventivas

Referencias:

Cissp Cert Guide (3ª Edición) Capítulo 7: Operaciones de seguridad, recuperación de confianza

Pregunta #158 de 163

Id. de pregunta: 1105536

Durante el próximo fin de semana, su equipo está programado para realizar pruebas que incluyen el cierre del sitio en vivo y llevar el sitio alternativo a la operación completa. ¿Qué prueba se realizará?

- ✗ **A)** prueba de recorrido estructurado
- ✗ **B)** prueba de simulación
- ✓ **C)** prueba de interrupción completa
- ✗ **D)** prueba paralela

Explicación

Una prueba de interrupción completa incluye apagar el sitio original y hacer que el sitio opcional esté completamente operativo. Esta prueba se considera la más intrusiva y requiere planificación y coordinación entre las partes involucradas. Esta prueba solo debe realizarse cuando todas las demás pruebas se han realizado y se han realizado correctamente.

La prueba de recorrido estructurado es una revisión del plan para asegurarse de que se incluyen todos los pasos. Una prueba de simulación es una ejecución práctica del plan de recuperación ante desastres para un escenario determinado. Una prueba paralela prueba sistemas específicos para garantizar el funcionamiento en instalaciones alternativas. Con una prueba paralela, se toman líneas de base de rendimiento para garantizar que el procesamiento todavía está en niveles aceptables.

Objetivo:
Operaciones de seguridad

Subobsecución:
Probar planes de recuperación ante desastres (DRP)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, prueba de interrupción completa

Pregunta #159 de 163

Id. de pregunta: 1105433

Su empresa tiene varios tipos diferentes de supervisión de red que utiliza para detectar y prevenir ataques de red. ¿Qué tipo de monitoreo tiene más probabilidades de producir una alerta falsa?

✓ **A)** basado en anomalías

✗ **B)** basado en la detección de uso indebido

✗ **C)** basado en firmas

✗ **D)** basado en el comportamiento

Explicación

Es más probable que la supervisión basada en anomalías produzca una alerta falsa. Con la supervisión basada en anomalías, se producen alertas donde hay desviaciones del comportamiento normal. Las desviaciones del comportamiento normal ocurrirán normalmente pero no siempre son indicaciones de un posible ataque. Con este tipo de monitoreo, hay un período de aprendizaje inicial antes de que se puedan detectar anomalías. Una vez establecidas las líneas de base, la supervisión basada en anomalías puede detectar anomalías. A veces, la línea de base se establece a través de un proceso manual.

La supervisión basada en la detección de uso indebido es la misma que la supervisión basada en firmas. Es más probable que la supervisión basada en firmas le proporcione una falsa sensación de seguridad en lugar de una alerta falsa. La supervisión basada en firmas se basa en una base de datos que contiene las identidades de posibles ataques. Esta base de datos se conoce como la base de datos de firmas. La supervisión basada en firmas vigila las intrusiones que coinciden con una identidad o firma conocida. La supervisión basada en firmas requiere que las actualizaciones se obtengan regularmente para garantizar la eficacia.

No es probable que la supervisión basada en el comportamiento produzca una alerta falsa porque ha definido un comportamiento no aceptable. Es más susceptible de darle una falsa sensación de seguridad. Es tan fuerte como los comportamientos que ha definido. Si no define correctamente los comportamientos inapropiados, pueden producirse ataques. La supervisión basada en el comportamiento busca un comportamiento que no está permitido y actúa en consecuencia. Cuando se define una regla que impide que un cliente de correo electrónico ejecute el comando cmd.exe y le avisa cuando se intenta, se utiliza la supervisión basada en el comportamiento.

Objetivo:
Operaciones de seguridad

Subobsecución:
Llevar a cabo actividades de registro y vigilancia

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 4: Ids de comunicación y seguridad de red

---

Pregunta #160 de 163

Pregunta con id.: 1111800

De acuerdo con el plan de continuidad del negocio, esta semana su equipo debe completar una prueba de sistemas específicos para garantizar su funcionamiento en instalaciones alternativas. Los resultados de la prueba deben compararse con el entorno vivo. ¿Qué prueba estás completando?

✗ **A)** prueba de interrupción completa

✗ **B)** prueba de recorrido estructurado

✗ **C)** prueba de simulación

✓ **D)** prueba paralela

Explicación

Una prueba paralela prueba sistemas específicos para garantizar el funcionamiento en instalaciones alternativas. Los resultados de esta prueba deben compararse con el sistema original para garantizar un funcionamiento lo más cercano posible a lo normal. Con una prueba paralela, se toman líneas de base de rendimiento para garantizar que el procesamiento todavía está en niveles aceptables.

La prueba de recorrido estructurado es una revisión del plan para asegurarse de que se incluyen todos los pasos.

Una prueba de simulación es una ejecución práctica del plan de recuperación ante desastres para un escenario determinado.

Una prueba de interrupción completa incluye apagar el sitio original y hacer que el sitio opcional esté completamente operativo. Esta prueba solo debe realizarse cuando todas las demás pruebas se han realizado y se han realizado correctamente. Mientras que una prueba paralela prueba la funcionalidad de procesamiento del sitio alternativo, la prueba de interrupción completa realmente replica un desastre al detener la producción.

Otra prueba de recuperación ante desastres es la lista de comprobación, que determina si se almacenan suficientes suministros en el sitio de copia de seguridad, si los listados de números de teléfono están actualizados, si las cantidades de formularios son adecuadas y si hay disponible una copia del plan de recuperación y los manuales operativos necesarios. Bajo esta técnica de prueba, el equipo de recuperación revisa el plan e identifica los componentes clave que deben estar disponibles. La prueba de lista de comprobación garantiza que la organización cumple con los requisitos del plan de recuperación ante desastres.

Una prueba de ejercicio de mesa se considera la forma más rentable y eficiente de identificar áreas de superposición en el plan antes de realizar ejercicios de entrenamiento más exigentes. Pero no se considera uno de los tipos de pruebas de recuperación ante desastres.

A continuación se muestra una lista de los tipos de pruebas de recuperación ante desastres, desde menos extensas hasta más extensas:

- Lista de verificación
- Recorrido estructurado
- Paralelo
- Simulación

- Interrupción total

Lo único que es seguro acerca de todos los planes de continuidad del negocio y planes de recuperación es que se vuelven obsoletos rápidamente. Por esta razón, la prueba y la revisión de algún tipo es vital. Los resultados más útiles para la administración son una lista de las operaciones correctas y no exitosas. Esto le dará a la administración la oportunidad de revisar las áreas problemáticas y corregirlas si es necesario. El plan debe revisarse según sea necesario para garantizar la recuperación satisfactoria de todas las funciones adicionales. Es importante probar los planes de recuperación ante desastres con frecuencia porque un plan no se considera viable hasta que se ha realizado una prueba. Si no se encuentran deficiencias durante una prueba, entonces la prueba probablemente fue defectuosa.

La prueba del plan de recuperación ante desastres debe completarse por las siguientes razones:

- Las pruebas comprueban la capacidad de procesamiento del sitio de copia de seguridad alternativo.
- La prueba prepara y entrena al personal para ejecutar sus deberes de la emergencia.
- Las pruebas identifican deficiencias en los procedimientos de recuperación.
- Las pruebas comprueban la precisión de los procedimientos de recuperación.

Durante un procedimiento de recuperación de prueba, un paso importante es mantener registros de eventos importantes que ocurren durante el procedimiento. Además, debe informar de los eventos a la administración.

Objetivo:
Operaciones de seguridad

Subobsecución:
Participar en la planificación y los ejercicios de continuidad del negocio (BC)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, prueba paralela

---

Pregunta #161 de 163

Id. de pregunta: 1114791

Debe documentar las directrices adecuadas que deben incluirse como parte de cualquier directiva de seguridad que implique al personal que viaja con dispositivos emitidos por la compañía. Se le ha dado una lista de posibles consejos para que los viajeros deben ser incluidos en las directrices de la siguiente manera:

R. La privacidad al viajar, sin importar el medio de conexión, no está garantizada.

B. Los movimientos de personal se pueden rastrear utilizando dispositivos móviles.

C. El software malintencionado se puede insertar en un dispositivo desde cualquier conexión controlada por otra persona o a través de unidades usb.

D. No lleve el dispositivo con usted si no lo necesita.

¿Qué consejos son consejos válidos que deben incluirse como parte de las directrices para el personal?

- ✗ **A)** Sólo B, C y D
- ✗ **B)** Sólo A, B y C
- ✗ **C)** Sólo A, C y D
- ✓ **D)** Todos los consejos

Explicación

Toda la lista de consejos son consejos válidos que deben incluirse como parte de las directrices para el personal que puede viajar con dispositivos emitidos por la compañía.

Otros consejos incluyen:

- Toda la información que usted transmite puede ser interceptada.
- Todas las personas están en riesgo, aunque algunas en posiciones corporativas o gubernamentales sensibles pueden estar en un riesgo más alto.
- Los delincuentes extranjeros son expertos en hacerse pasar por alguien de confianza para obtener información sensible.
- Si alguna vez se examina el dispositivo o se deja en una habitación de hotel cuando se examina la habitación, suponga que el disco duro se ha copiado y el dispositivo se ha comprometido.

Objetivo:
Operaciones de seguridad

Subobsecución:
Abordar las preocupaciones de seguridad y protección del personal

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, viajes

---

Pregunta #162 de 163

Id. de pregunta: 1105525

Debe asegurarse de que se puedan recuperar todos los sistemas, redes y aplicaciones principales. ¿Qué debe crear o realizar?

- ✗ **A)** análisis del riesgo
- ✗ **B)** análisis de vulnerabilidades

✓ **C)** plan de contingencia

✗ **D)** análisis de impacto en el negocio (BIA)

Explicación

El plan de contingencia se crea para garantizar que se puedan recuperar todos los sistemas, redes y aplicaciones principales. Debería crearse un plan para situaciones imprevistas para cada entidad principal, incluidas todas las entidades de equipo y programas informáticos.

Un análisis de vulnerabilidades identifica las vulnerabilidades de su empresa. Forma parte del plan de continuidad del negocio.

Un análisis de riesgos es parte del análisis de impacto en el negocio (BIA). Se utiliza para calcular el riesgo para descubrir qué funciones ofrecerían la mayor pérdida financiera a la empresa.

Se crea un BIA para identificar las funciones vitales y priorizarlas en función de la necesidad. Se identifican las vulnerabilidades y amenazas, y se calculan los riesgos.

Un plan de contingencia aborda todos los riesgos potenciales, residuales e identificados. Los riesgos generalmente se identifican mediante la investigación sobre los tipos de sistemas existentes.

Un error en el plan de contingencia suele ser el resultado de un error de gestión.

La persona designada para gestionar el proceso de planificación para imprevistos debe proporcionar orientación al personal directivo superior. Además, esta persona debe garantizar la identificación de todas las funciones empresariales críticas e integrar el proceso de planificación en todas las unidades de negocio. Cuando cualquier parte de la LAN no está alojada internamente y forma parte de un entorno de servidor de creación, es responsabilidad del planificador de contingencia identificar al administrador del servidor de creación, identificar para él el período de tiempo de recuperación necesario para las aplicaciones empresariales, obtener una copia de los procedimientos de recuperación y participar en la validación de las pruebas del servidor del edificio.

Objetivo:
Operaciones de seguridad

Subobsecución:
Implementar procesos de recuperación ante desastres (DR)

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 1: Seguridad y Gestión de Riesgos, Plan de Contingencia

---

Pregunta #163 de 163

Id. de pregunta: 1105472

Según la directiva de copia de seguridad de datos de su organización, debe realizar un seguimiento del número y la ubicación de las versiones de copia de seguridad de los datos de la organización. ¿Cuál es el objetivo principal de esta actividad?

- ✗ **A)** Para crear una pista de auditoría
- ✓ **B)** para garantizar la eliminación adecuada de la información
- ✗ **C)** para demostrar la diligencia debida
- ✗ **D)** Para restringir el acceso a las versiones de copia de seguridad

Explicación

El objetivo principal de realizar un seguimiento del número y la ubicación de las versiones de copia de seguridad es garantizar la eliminación adecuada de la información.

Para restringir el acceso a la versión de copia de seguridad, debe implementar los controles físicos y de acceso adecuados.

Para crear un seguimiento de auditoría, debe habilitar el registro de eventos o auditoría.

Para demostrar la diligencia debida, debe conservar los registros de eventos y auditoría.

Objetivo:
Operaciones de seguridad

Subobsecución:
Comprender y aplicar conceptos fundamentales de operaciones de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, estrategias de almacenamiento de copia de seguridad