ExecuTrain

Impulsamos tu talento tecnológico

MICROSOFT

RED HAT

VIRTUALIZACIÓN

CIBERSEGURIDAD

DESARROLLO

OFFICE

BIG DATA

BLOCK CHAIN

BASES DE DATOS

GESTIÓN DE SERVICIOS IT

CLOUD COMPUTING

METODOLOGÍAS EN PROYECTOS

SISTEMAS OPERATIVOS

Y MÁS...

www.executrain.com.mx

¿Por qué ExecuTrain?

ExecuTrain es un proveedor de entrenamiento corporativo a nivel internacional y líder mundial en la capacitación empresarial. Contamos con más de 30 años de Experiencia y con más de 75 mil personas capacitadas a nivel Nacional.

Te guiamos en la definición de tus requerimientos de capacitación, en las diferentes etapas:

- ✓ Detección de necesidades, evaluación de conocimientos, plan de capacitación y seguimiento posterior para elegir el plan de capacitación como tú lo necesitas.
- ✓ El **más amplio catálogo de cursos**, desde un nivel básico hasta los niveles de conocimientos más especializados.
- ✓ En ExecuTrain el material y la **metodología están diseñados por expertos en aprendizaje humano**. Lo que te garantiza un mejor conocimiento en menor tiempo.
- ✓ Tú puedes confiar y estar seguro del aprendizaje porque nuestro **staff de instructores es de primer nivel**, algunos de los cuales son consultores en reconocidas empresas.
- ✓ No pierdas tu tiempo, los cursos están diseñados para un aprendizaje práctico.

Nuestro compromiso es que tú aprendas, si no quedas satisfecho con los resultados del programa, podrás volver a tomar los cursos hasta tu entera satisfacción o la devolución de tu dinero.

Modalidad de Servicio

Cursos en Fecha Calendario

Súmate a nuestros grupos en fechas públicas.

Cursos Privados

On site, en nuestras instalaciones o en línea con instructor en vivo.

Autoestudio con soporte de instructor

Cursos en modalidad autoestudio, con acceso 24/7 a la plataforma de estudio, con soporte de instructor y foros de ayuda

ExecuTrain
Impulsamos tu talento tecnológico

Duración: 28 horas

SC-100 / Microsoft Cybersecurity Architect

Se trata de un curso avanzado de nivel de experto. Aunque no es necesario asistir, se recomienda encarecidamente que los alumnos hayan aprobado otra certificación de nivel de técnico auxiliar en la cartera seguridad, cumplimiento e identidad (como AZ-500, SC-200 o SC-300) antes de asistir a esta clase. Este curso prepara a los alumnos con la experiencia para diseñar y evaluar estrategias de ciberseguridad en las siguientes áreas: Confianza cero; gobernanza, riesgo y cumplimiento (GRC), operaciones de seguridad (SecOps) y datos y aplicaciones. Los alumnos también aprenderán a diseñar soluciones siguiendo los principios de confianza cero y a especificar los requisitos de seguridad para la infraestructura en la nube en diferentes modelos de servicio (SaaS, PaaS, IaaS).

Perfil del Público

Este curso es para ingenieros de seguridad en la nube con experiencia que han aprobado una certificación anterior en la cartera seguridad, cumplimiento e identidad. Concretamente, los alumnos deben tener experiencia y conocimientos avanzados en una amplia gama de áreas de ingeniería de seguridad, como la identidad y el acceso, la protección de plataformas, las operaciones de seguridad, la protección de datos y la protección de aplicaciones. También deben tener experiencia con implementaciones híbridas y en la nube. En su lugar, los alumnos principiantes deben realizar el curso SC-900: Conceptos básicos de seguridad, cumplimiento e identidad de Microsoft.

Rol de trabajo: Arquitecto de soluciones
Preparación para el examen: SC-100

Requisitos Previos

Antes de asistir a este curso, los estudiantes deben tener:

- ✓ Se recomienda encarecidamente haber asistido y superado una de las certificaciones de nivel asociado en la cartera de seguridad, cumplimiento e identidad (como AZ-500, SC-200 o SC-300)
- ✓ Experiencia avanzada y conocimientos sobre la identidad y el acceso, la protección de plataformas, las operaciones de seguridad, la protección de datos y la protección de aplicaciones.
- ✓ Experiencia en implementaciones híbridas y en la nube.

Módulos

Creación de una estrategia y una arquitectura de seguridad general

Aprenda a crear una estrategia y una arquitectura de seguridad general teniendo en cuenta la confianza cero.

Objetivos de aprendizaje

Al final de este módulo, podrá hacer lo siguiente:

- Desarrollo de puntos de integración en una arquitectura
- Desarrollo de requisitos de seguridad basados en objetivos comerciales
- Traducción de los requisitos de seguridad en capacidades técnicas
- Diseño de la seguridad para una estrategia de resistencia
- Diseño de una estrategia de seguridad para entornos híbridos y multiinquilino
- Diseño de estrategias técnicas y de gobernanza para el filtrado y la segmentación del tráfico

Diseño de una estrategia de operaciones de

Aprenda a diseñar una estrategia de ciberseguridad para las operaciones de seguridad (SecOps).

Objetivos de aprendizaje

Al final de este módulo, podrá hacer lo siguiente:

- Diseñar una estrategia de seguridad de registro y auditoría.
- Desarrollar operaciones de seguridad para entornos híbridos y de varias nubes.
- Diseñar una estrategia para la Administración de eventos e información de seguridad (SIEM) y la orquestación, la automatización y la respuesta de seguridad (SOAR).
- Evaluar flujos de trabajo de seguridad.
- Revisar las estrategias de seguridad para la administración de incidentes.
- Evaluar las operaciones de seguridad para la inteligencia técnica sobre amenazas.
- Supervisar orígenes para obtener información sobre amenazas y mitigaciones.

Diseño de una estrategia de seguridad de identidad

Aprenda a diseñar una estrategia de ciberseguridad para la administración de identidades.

Objetivos de aprendizaje

Al final de este módulo, podrá hacer lo siguiente:

- Recomendar un almacén de identidades para la seguridad.
- Recomendar estrategias de autenticación segura y autorización de seguridad.
- Proteger el acceso condicional.
- Diseñar una estrategia para la asignación y la delegación de roles.
- Definir la gobernanza de identidades para las revisiones de acceso y la administración de derechos.
- Diseñar una estrategia de seguridad para el acceso de roles con privilegios a la infraestructura.
- Diseñar una estrategia de seguridad para el acceso con privilegiados.

Evaluación de una estrategia de cumplimiento normativo

Descubra cómo evaluar una estrategia de ciberseguridad para el cumplimiento normativo.

Objetivos de aprendizaje

Al final de este módulo, podrá hacer lo siguiente:

- Interprete los requisitos de cumplimiento y sus funcionalidades técnicas.
- Evalúe el cumplimiento de la infraestructura mediante Microsoft Defender for Cloud.
- Interprete las puntuaciones de cumplimiento y recomiende acciones para resolver problemas o mejorar la seguridad.
- Diseñe y valide la implementación de Azure Policy.
- Realice diseños para requisitos de residencia de datos.
- Traduzca los requisitos de privacidad en los requisitos de las soluciones de seguridad.

Evaluación de la posición de seguridad y recomendación de estrategias técnicas para administrar el riesgo

Aprenda a evaluar la posición de seguridad de una organización y recomendar estrategias técnicas para administrar el riesgo.

Objetivos de aprendizaje

Al final de este módulo, podrá hacer lo siguiente:

- Evaluar las posiciones de seguridad mediante puntos de referencia.
- Evaluar las posiciones de seguridad con Microsoft Defender for Cloud.
- Evaluar las posiciones de seguridad mediante puntuaciones de seguridad.
- Evaluar la higiene de seguridad de las cargas de trabajo en la nube.
- Diseñar la seguridad de una zona de aterrizaje de Azure.

Interpretar la inteligencia técnica sobre amenazas y recomendar medidas para mitigar el riesgo.

- Recomendar características o controles de seguridad para mitigar los riesgos identificados

Descripción de los procedimientos recomendados para la arquitectura y cómo cambian con la nube

Aprenda los procedimientos recomendados para la arquitectura de ciberseguridad y cómo se han visto afectadas por la informática en la nube.

Objetivos de aprendizaje

Al final de este módulo, podrá hacer lo siguiente:

- Planificar e implementar una estrategia de seguridad entre equipos.
- Establecer una estrategia y un proceso para la evolución proactiva y continua de una estrategia de seguridad.

Diseño de una estrategia para proteger los puntos de conexión de cliente y servidor

Aprenda a diseñar una estrategia de ciberseguridad para proteger los puntos de conexión de cliente y servidor.

Objetivos de aprendizaje

Al final de este módulo, podrá hacer lo siguiente:

- Diseñar una estrategia de seguridad de registro y auditoría.
- Desarrollar operaciones de seguridad para entornos híbridos y multinube
- Diseñar una estrategia para la Administración de eventos e información de seguridad (SIEM) y la orquestación, la automatización y la respuesta de seguridad (SOAR).
- Evaluar flujos de trabajo de seguridad.
- Revisar las estrategias de seguridad para la administración de incidentes.

- Evaluar las operaciones de seguridad para la inteligencia técnica sobre amenazas.
- Supervisar orígenes para obtener información sobre amenazas y mitigaciones.

Diseño de una estrategia para proteger los servicios PaaS, IaaS y SaaS

Descubra cómo diseñar una estrategia de ciberseguridad que protegerá los servicios en la nube en los modelos de servicio SaaS, PaaS e IaaS.

Objetivos de aprendizaje

Al final de este módulo, podrá hacer lo siguiente:

- Especifique las líneas base de seguridad para los servicios SaaS, PaaS e IaaS.
- Especifique los requisitos de seguridad para cargas de trabajo web, almacenamiento, datos e IoT.
- Especifique los requisitos de seguridad para los contenedores y la orquestación de contenedores.

Especificación de los requisitos de seguridad para aplicaciones

Descubra cómo especificar los requisitos de ciberseguridad para aplicaciones.

Objetivos de aprendizaje

Al final de este módulo, podrá hacer lo siguiente:

- Especifique las prioridades para mitigar las amenazas a las aplicaciones.
- Especifique un estándar de seguridad para incorporar una nueva aplicación.
- Especifique una estrategia de seguridad para aplicaciones y API.

Diseño de una estrategia para proteger los datos

Descubra cómo diseñar una estrategia de ciberseguridad para proteger los datos.

Objetivos de aprendizaje

Al final de este módulo, podrá hacer lo siguiente:

- Especifique prioridades para mitigar las amenazas a los datos.
- Diseñe una estrategia para identificar y proteger datos confidenciales.
- Especifique un estándar de cifrado para los datos en reposo y en movimiento.

Recomendación de procedimientos de seguridad mediante arquitecturas de referencia de ciberseguridad de Microsoft (MCRA) y pruebas comparativas de seguridad de Microsoft Cloud

Aprenderá a usar las instrucciones de las arquitecturas de referencia de ciberseguridad de Microsoft y las pruebas comparativas de seguridad de Microsoft Cloud para ayudar a una organización a aplicar los principios de Confianza cero y proteger su infraestructura.

Objetivos de aprendizaje

En este módulo aprenderá a:

- Usar la arquitectura de referencia de ciberseguridad de Microsoft (MCRA) para recomendar procedimientos de seguridad
- Uso de pruebas comparativas de seguridad de Microsoft Cloud para recomendar procedimientos de seguridad
- Usar el plan de modernización rápida de Confianza cero (RaMP) para recomendar una estrategia para actualizar la seguridad de la organización

Recomendar una metodología segura mediante Cloud Adoption Framework (CAF)

Aprenderá a usar Cloud Adoption Framework para recomendar procedimientos recomendados de seguridad que ayuden a una organización a pasarse a la nube a la vez que mejora la posición de seguridad general.

Objetivos de aprendizaje

En este módulo aprenderá a:

- Recomendar un proceso de DevSecOps
- Recomendar una metodología de protección de recursos
- Recomendar estrategias para administrar y minimizar el riesgo

Recomendar una estrategia de ransomware mediante procedimientos recomendados de seguridad de Microsoft

Aprenderá a ejecutar las tres fases importantes de la protección contra ransomware: crear un plan de recuperación, limitar el ámbito de daño y hacer que sea difícil que se cuele malware.

Objetivos de aprendizaje

En este módulo aprenderá a:

- Reconocer diferentes tipos de ransomware
- Ayudar a una organización a mitigar el riesgo de un ataque de ransomware mediante la creación de un plan de recuperación
- Ayudar a una organización a mitigar el riesgo de un ataque de ransomware limitando el ámbito de daño
- Ayudar a una organización a mitigar el riesgo de un ataque de ransomware mediante la protección de los elementos clave de la infraestructura