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: 35 horas

MS-102 / Microsoft 365 Administrator Essentials

En este curso se tratan los siguientes elementos clave de la administración de Microsoft 365: administración de inquilinos, sincronización de identidades y seguridad y cumplimiento.

En la administración de inquilinos de Microsoft 365, aprenderá cómo configurar su inquilino de Microsoft 365, incluido su perfil de organización, opciones de suscripción de inquilino, servicios de componentes, cuentas y licencias de usuario, grupos de seguridad y roles administrativos. A continuación, realizará la transición a la configuración de Microsoft 365, con un enfoque principal en la configuración de la conectividad de cliente de Office. Por último, verá cómo administrar las instalaciones de cliente controladas por el usuario de implementaciones de Aplicaciones de Microsoft 365 para empresas.

A continuación, se pasa a un examen detallado de la sincronización de identidades de Microsoft 365, con un enfoque en Azure Active Directory Connect y Connect Cloud Sync. Aprenderá a planificar e implementar cada una de estas opciones de sincronización de directorios, cómo administrar identidades sincronizadas y cómo implementar la administración de contraseñas en Microsoft 365 mediante la autenticación multifactor y la administración de contraseñas de autoservicio.

En la parte de administración de seguridad de Microsoft 365, comenzamos por examinar los tipos habituales de vectores de amenazas y filtraciones de datos a los que se enfrentan hoy en día las organizaciones. A continuación, verá cómo las soluciones de seguridad de Microsoft 365 abordan cada una de estas amenazas. Se le presentará Microsoft Secure Score y Azure Active Directory Identity Protection. Luego aprenderá a administrar los servicios de seguridad de Microsoft 365, incluidos Exchange Online Protection, Safe Attachments, y Safe Links. Finalmente, se le presentarán los diversos informes que supervisan el estado de seguridad de una organización. Después, pasará de los servicios de seguridad a la inteligencia sobre amenazas; específicamente, mediante Microsoft 365 Defender, las aplicaciones de Microsoft Defender for Cloud y Microsoft Defender para punto de conexión.

Perfil del Público

Este curso está diseñado para personas que aspiran a la función de administrador de Microsoft 365 Enterprise y han completado, como mínimo, una de las rutas de certificación de administrador basadas en roles de Microsoft 365.

Rol de trabajo: Administrador
Preparación para el examen: MS-102

Requisitos Previos

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

- ✓ Un curso de administrador basado en roles, como Mensajería, Trabajo en equipo, Seguridad y cumplimiento, o Colaboración.
- ✓ Conocimiento competente de DNS y experiencia funcional básica con los servicios de Microsoft 365.
- ✓ Un conocimiento competente de las prácticas generales de TI.
- ✓ Conocimientos prácticos de PowerShell

Módulos

Configura tu experiencia de Microsoft 365

Este módulo examina cada una de las tareas que una organización debe completar para configurar correctamente su experiencia de Microsoft 365.

Objetivos de aprendizaje

Al final de este módulo, usted debería ser capaz de:

- Configure el perfil de la organización de su empresa, que es esencial para configurar el inquilino de su empresa.
- Mantenga los requisitos mínimos de suscripción para su empresa.
- Administre sus servicios y complementos asignando más licencias, comprando más almacenamiento, etc.
- Cree una lista de verificación que le permita confirmar que su arrendatario de Microsoft 365 cumple con sus necesidades comerciales.

Administrar usuarios, contactos y licencias en Microsoft 365

Este módulo brinda instrucciones sobre cómo administrar cuentas de usuario y licencias en Microsoft 365, crear y administrar cuentas de usuario, asignar licencias de Microsoft 365 a usuarios y recuperar cuentas de usuario eliminadas.

Objetivos de aprendizaje

Al final de este módulo, usted debería ser capaz de:

- Identifique qué modelo de identidad de usuario se adapta mejor a su organización.
- Cree cuentas de usuario desde el Centro de administración de Microsoft 365 y Windows PowerShell.
- Administre cuentas de usuario y licencias en Microsoft 365.
- Recuperar cuentas de usuario eliminadas en Microsoft 365.
- Realice un mantenimiento masivo de usuarios en Azure Active Directory.

Administrar grupos en Microsoft 365

Este módulo brinda instrucciones sobre cómo crear grupos para distribuir correo electrónico a múltiples usuarios dentro de Exchange Online. También explica cómo crear grupos para admitir la colaboración en SharePoint Online.

Objetivos de aprendizaje

Al final de este módulo, usted debería ser capaz de:

- Describir los distintos tipos de grupos disponibles en Microsoft 365.
- Cree y administre grupos con el centro de administración de Microsoft 365 y Windows PowerShell.
- Cree y administre grupos en Exchange Online y SharePoint Online.

Agregar un dominio personalizado en Microsoft 365

Este módulo proporciona instrucciones sobre cómo agregar un dominio personalizado a su implementación de Microsoft 365. También examina los requisitos de DNS que son necesarios para admitir un nuevo dominio.

Objetivos de aprendizaje

Al final de este módulo, usted debería ser capaz de:

- Identifique los factores que deben tenerse en cuenta al agregar un dominio personalizado a Microsoft 365.
- Planifique las zonas DNS utilizadas en un dominio personalizado.
- Planifique los requisitos de registro de DNS para un dominio personalizado.
- Agregue un dominio personalizado a su implementación de Microsoft 365.

Configurar la conectividad del cliente con Microsoft 365

Este módulo examina cómo los clientes se conectan a Microsoft 365. También proporciona instrucciones

sobre cómo configurar la resolución de nombres y los clientes de Outlook, y cómo solucionar problemas de conectividad del cliente.

Objetivos de aprendizaje

Al final de este módulo, usted debería ser capaz de:

- Describir cómo Outlook usa la detección automática para conectar un cliente de Outlook a Exchange Online.
- Identifique los registros DNS necesarios para que Outlook y otros clientes relacionados con Office ubiquen automáticamente los servicios en Microsoft 365 mediante el proceso de detección automática.
- Describir los protocolos de conectividad que permiten que Outlook se conecte a Microsoft 365.
- Identifique las herramientas que pueden ayudarlo a solucionar problemas de conectividad en las implementaciones de Microsoft 365.

Configurar roles administrativos en Microsoft 365

Este módulo examina la funcionalidad clave que está disponible en los roles de administrador de Microsoft 365 más utilizados. También proporciona instrucciones sobre cómo configurar estos roles.

Objetivos de aprendizaje

Al final de este módulo, usted debería ser capaz de:

- Describir el modelo de permisos de Azure RBAC que se usa en Microsoft 365.
- Describir los roles de administrador de Microsoft 365 más comunes.
- Identifique las tareas clave asignadas a los roles de administrador comunes de Microsoft 365.
- Delegue roles de administrador a los socios.
- Administre permisos usando unidades administrativas en Azure Active Directory.
- Eleve los privilegios para acceder a los centros de administración mediante Azure AD Privileged Identity Management.

Administrar el estado y los servicios de los inquilinos en Microsoft 365

Este módulo examina cómo monitorear la transición de su organización a Microsoft 365 usando las herramientas de Microsoft 365. También examina cómo desarrollar un plan de respuesta a incidentes y solicitar asistencia de Microsoft.

Objetivos de aprendizaje

Al final de este módulo, usted debería ser capaz de:

- Supervise el estado del servicio de Microsoft 365 de su organización en el Centro de administración de Microsoft 365.
- Desarrolle un plan de respuesta a incidentes para tratar los incidentes que puedan ocurrir con su servicio de Microsoft 365.
- Solicite asistencia de Microsoft para abordar problemas técnicos, de preventa, de facturación y de soporte de suscripción.

Implementar aplicaciones de Microsoft 365 para empresas

Este módulo examina cómo implementar las aplicaciones de Microsoft 365 para la suite de productividad empresarial en implementaciones centralizadas y dirigidas por el usuario.

Objetivos de aprendizaje

Al final de este módulo, usted debería ser capaz de:

- Describir las aplicaciones de Microsoft 365 para la funcionalidad empresarial.
- Configure el kit de herramientas de preparación.
- Planifique una estrategia de implementación para Aplicaciones de Microsoft 365 para empresas.
- Complete una instalación dirigida por el usuario de Aplicaciones de Microsoft 365 para empresas.
- Implemente Aplicaciones de Microsoft 365 para empresas con Microsoft Endpoint Configuration Manager.

- Identificar los mecanismos para administrar implementaciones centralizadas de Aplicaciones de Microsoft 365 para empresas.
- Implemente Aplicaciones de Microsoft 365 para empresas con Office Deployment Toolkit.
- Describir cómo administrar Aplicaciones de Microsoft 365 para actualizaciones empresariales.
- Determine qué canal de actualización y método de aplicación se aplica a su organización.

Analice los datos de su lugar de trabajo de Microsoft 365 con Microsoft Viva Insights

Este módulo examina las características analíticas del lugar de trabajo de Microsoft Viva Insights, incluido cómo funciona y cómo genera información y mejora la colaboración dentro de una organización.

Objetivos de aprendizaje

Después de completar este módulo, debería ser capaz de:

- Identifique cómo Microsoft Viva Insights puede ayudar a mejorar los comportamientos de colaboración en su organización.
- Descubra las fuentes de datos utilizadas en Microsoft Viva Insights.
- Explicar los conocimientos de alto nivel disponibles a través de Microsoft Viva Insights.
- Cree análisis personalizados con Microsoft Viva Insights.
- Resuma las tareas y consideraciones para configurar Microsoft Viva Insights y administrar la privacidad.

Explore la sincronización de identidades

Este módulo examina la sincronización de identidades y explora las opciones de autenticación y aprovisionamiento que se pueden usar, y el funcionamiento interno de la sincronización de directorios.

Objetivos de aprendizaje

Al final de este módulo, usted debería ser capaz de:

- Describir las opciones de autenticación y aprovisionamiento de Microsoft 365
- Explicar los dos modelos de identidad en Microsoft 365: identidad solo en la nube e identidad híbrida
- Explicar los tres métodos de autenticación en el modelo de identidad híbrida: sincronización de hash de contraseña, autenticación de paso y autenticación federada
- Describir cómo Microsoft 365 usa comúnmente la sincronización de directorios

Prepárese para la sincronización de identidad con Microsoft 365

Este módulo examina todos los aspectos de planificación que deben tenerse en cuenta al implementar la sincronización de directorios entre Active Directory local y Microsoft 365.

Objetivos de aprendizaje

Al final de este módulo, usted debería ser capaz de:

- Identifique las tareas necesarias para configurar su entorno de Azure Active Directory.
- Planifique la sincronización de directorios para sincronizar sus objetos de Active Directory locales con Azure AD.
- Identificar las características de la sincronización de Azure AD Connect y la sincronización en la nube de Azure AD Connect.
- Elija qué sincronización de directorios se adapta mejor a su entorno y necesidades comerciales.

Implementar herramientas de sincronización de directorios

Este módulo examina los requisitos de instalación de Azure AD Connect y Azure AD Connect Cloud Sync, las opciones para instalar y configurar las herramientas y cómo monitorear los servicios de sincronización usando Azure AD Connect Health.

Objetivos de aprendizaje

Al final de este módulo, debería ser capaz de:

- Configurar los requisitos previos de Azure AD Connect y Azure AD Connect Cloud Sync
- Configurar Azure AD Connect y Azure AD Connect Cloud Sync
- Supervise los servicios de sincronización con Azure AD Connect Health

Administrar identidades sincronizadas

Este módulo examina cómo administrar las identidades de los usuarios cuando se configura Azure AD Connect, cómo administrar usuarios y grupos en Microsoft 365 con Azure AD Connect y cómo mantener la sincronización de directorios.

Objetivos de aprendizaje

Al final de este módulo, usted debería ser capaz de:

- Asegúrese de que los usuarios se sincronicen de manera eficiente
- Administrar grupos con sincronización de directorios
- Use Azure AD Connect Sync Security Groups para ayudar a mantener la sincronización de directorios
- Configurar filtros de objetos para la sincronización de directorios
- Solucionar problemas de sincronización de directorios mediante varias tareas y herramientas de solución de problemas

Administrar el acceso seguro de los usuarios en Microsoft 365

Este módulo examina varias tareas relacionadas con contraseñas para usuarios y administradores, que incluyen:

- creación y configuración de políticas de contraseñas
- configurar la administración de contraseñas de autoservicio
- configurar la autenticación multifactor
- implementar paquetes de derechos
- implementar políticas de acceso condicional
- Objetivos de aprendizaje

Al final de este módulo, usted debería ser capaz de:

- Administrar contraseñas de usuario
- Describir la autenticación de paso
- Habilitar la autenticación multifactor
- Describir la gestión de contraseñas de autoservicio
- Implementar el bloqueo inteligente de Azure AD
- Implementar paquetes de derechos en Azure AD Identity Governance
- Implementar políticas de acceso condicional
- Crear y realizar una revisión de acceso

Examine los vectores de amenazas y las filtraciones de datos

Este módulo examina los tipos de vectores de amenazas y sus posibles resultados con los que las organizaciones deben lidiar a diario y cómo los usuarios pueden permitir que los piratas informáticos accedan a los objetivos mediante la ejecución inadvertida de contenido malicioso.

Objetivos de aprendizaje

Al final de este módulo, usted debería ser capaz de:

- Describir las técnicas que utilizan los piratas informáticos para comprometer las cuentas de los usuarios a través del correo electrónico.
- Describir las técnicas que utilizan los piratas informáticos para obtener control sobre los recursos.
- Describir las técnicas que utilizan los piratas informáticos para comprometer los datos.
- Mitigar una violación de cuenta
- Evitar un ataque de elevación de privilegios
- Evite la exfiltración, la eliminación y el derrame de datos

Explore el modelo de seguridad Zero Trust

Este módulo examina los conceptos y principios del modelo de seguridad Zero Trust, así como también cómo Microsoft 365 lo admite y cómo su organización puede implementarlo.

Objetivos de aprendizaje

Al final de este módulo, usted debería ser capaz de:

- Describir el enfoque Zero Trust para la seguridad en Microsoft 365
- Describir los principios y componentes del modelo de seguridad Zero Trust
- Describa los cinco pasos para implementar un modelo de seguridad Zero Trust en su organización
- Explicar la historia y la estrategia de Microsoft en torno a las redes Zero Trust

Explore las soluciones de seguridad en Microsoft 365 Defender

Este módulo le presenta varias características de Microsoft 365 que pueden ayudar a proteger su organización contra amenazas cibernéticas, detectar cuándo un usuario o una computadora se ha visto comprometida y monitorear su organización en busca de actividades sospechosas.

Objetivos de aprendizaje

Al final de este módulo, usted debería ser capaz de:

- Identificar las funciones de Microsoft Defender para Office 365 que mejoran la seguridad del correo electrónico en una implementación de Microsoft 365
- Explicar cómo Microsoft Defender for Identity identifica, detecta e investiga amenazas avanzadas, identidades comprometidas y acciones internas maliciosas dirigidas a su organización.
- Explicar cómo Microsoft Defender para Endpoint ayuda a las redes empresariales a prevenir, detectar, investigar y responder a amenazas avanzadas.
- Describir cómo Microsoft 365 Threat Intelligence puede ser beneficioso para los responsables y administradores de seguridad de su organización
- Describa cómo Microsoft Cloud App Security mejora la visibilidad y el control sobre su arrendatario de Microsoft 365 a través de tres áreas principales

Examinar la puntuación segura de Microsoft

Este módulo examina cómo Microsoft Secure Score ayuda a las organizaciones a comprender lo que han hecho para reducir el riesgo de sus datos y les muestra lo que pueden hacer para reducir aún más ese riesgo.

Objetivos de aprendizaje

Al final de este módulo, usted debería ser capaz de:

- Describir los beneficios de Secure Score y qué tipo de servicios se pueden analizar
- Describir cómo recopilar datos utilizando la API Secure Score
- Describa cómo usar la herramienta para identificar brechas entre su estado actual y dónde le gustaría estar con respecto a la seguridad.
- Identifique acciones que aumenten su seguridad mitigando riesgos
- Explicar dónde buscar para determinar las amenazas que mitiga cada acción y el impacto que tiene en los usuarios.

Examinar la gestión de identidad privilegiada

Este módulo examina cómo Privileged Identity Management garantiza que los usuarios de su organización tengan los privilegios adecuados para realizar las tareas que necesitan realizar.

Objetivos de aprendizaje

Al final de este módulo, usted debería ser capaz de:

- Describa cómo Privileged Identity Management le permite administrar, controlar y monitorear el acceso a recursos importantes en su organización
- Configure la administración de identidades privilegiadas para su uso en su organización
- Describir cómo el historial de auditoría de Privileged Identity Management le permite ver todas las asignaciones y activaciones de usuarios dentro de un período de tiempo determinado para todos los roles privilegiados.

- Explicar cómo Microsoft Identity Manager ayuda a las organizaciones a administrar los usuarios, las credenciales, las políticas y el acceso dentro de sus organizaciones y entornos híbridos.
- Explicar cómo Privileged Access Management proporciona control de acceso granular sobre tareas de administración privilegiadas en Microsoft 365

Examine la protección de identidad de Azure

Este módulo examina cómo Azure Identity Protection proporciona a las organizaciones los mismos sistemas de protección que utiliza Microsoft para proteger las identidades.

Objetivos de aprendizaje

Al final de este módulo, usted debería ser capaz de:

- Describir Azure Identity Protection (AIP) y qué tipo de identidades se pueden proteger
- Habilite las tres políticas de protección predeterminadas en AIP
- Identificar las vulnerabilidades y eventos de riesgo detectados por AIP
- Planifique su investigación para proteger las identidades basadas en la nube
- Planifique cómo proteger su entorno de Azure Active Directory de infracciones de seguridad

Examinar la protección en línea de Exchange

Este módulo examina cómo Exchange Online Protection (EOP) protege a las organizaciones contra el phishing y la suplantación de identidad. También explora cómo EOP bloquea el spam, el correo electrónico masivo y el malware antes de que lleguen a los buzones de correo de los usuarios.

Objetivos de aprendizaje

Al final de este módulo, usted debería ser capaz de:

- Describa cómo Exchange Online Protection analiza el correo electrónico para proporcionar protección de canalización antimalware.
- Enumere varios mecanismos utilizados por Exchange Online Protection para filtrar correo no deseado y malware.
- Describa otras soluciones que los administradores pueden implementar para brindar protección adicional contra el phishing y la suplantación de identidad.
- Comprenda cómo EOP brinda protección contra el correo no deseado saliente.

Examine Microsoft Defender para Office 365

Este módulo examina cómo Microsoft Defender para Office 365 amplía la protección EOP mediante el filtrado de ataques dirigidos, como ataques de día cero en archivos adjuntos de correo electrónico y documentos de Office, y la protección en el momento del clic contra direcciones URL maliciosas.

Objetivos de aprendizaje

Al final de este módulo, debería ser capaz de:

- Describa cómo la función Datos adjuntos seguros en Microsoft Defender para Office 365 bloquea el malware de día cero en documentos y datos adjuntos de correo electrónico.
- Describir cómo la función Vínculos seguros en Microsoft Defender para Office 365 protege a los usuarios de direcciones URL maliciosas incrustadas en correos electrónicos y documentos que apuntan a sitios web maliciosos.
- Cree políticas de filtrado de spam saliente.
- Desbloquee a los usuarios que violaron las políticas de filtrado de spam para que puedan reanudar el envío de correos electrónicos.

Administración de datos adjuntos seguros

En este módulo se examina cómo administrar datos adjuntos seguros en el inquilino de Microsoft 365 mediante la creación y configuración de directivas y el uso de reglas de transporte para deshabilitar que una directiva surta efecto en determinados escenarios.

Objetivos de aprendizaje

Al final de este módulo, será capaz de lo siguiente:

- Creación y modificación de una directiva de datos adjuntos seguros mediante Microsoft 365 Defender
- Creación de una directiva de datos adjuntos seguros mediante PowerShell
- Configurar una directiva de Datos adjuntos seguros
- Describir cómo una regla de transporte puede deshabilitar una directiva de datos adjuntos seguros
- Describir la experiencia del usuario final cuando se examina un archivo adjunto de correo electrónico y se detecta que es malintencionado

Administrar Vínculos seguros

En este módulo se describe cómo administrar Vínculos seguros en el inquilino mediante la creación y configuración de directivas y el uso de reglas de transporte para deshabilitar la aplicación de una directiva en determinados escenarios.

Objetivos de aprendizaje

Al final de este módulo, será capaz de lo siguiente:

- Crear y modificar una directiva de vínculos seguros mediante Microsoft 365 Defender
- Crear una directiva de Vínculos seguros mediante PowerShell
- Configurar una directiva de vínculos seguros
- Describir cómo una regla de transporte puede deshabilitar una directiva de Vínculos seguros
- Describir la experiencia del usuario final cuando Vínculos seguros identifica un vínculo a un sitio web malintencionado insertado en el correo electrónico y un vínculo a un archivo malintencionado hospedado en un sitio web.

Explore la inteligencia de amenazas en Microsoft 365 Defender

Este módulo examina cómo Microsoft 365 Threat Intelligence proporciona a los administradores conocimientos basados en evidencia y consejos prácticos que se pueden usar para tomar decisiones informadas sobre la protección y la respuesta a los ataques cibernéticos contra sus inquilinos.

Objetivos de aprendizaje

Al final de este módulo, usted debería ser capaz de:

- Describir cómo la inteligencia de amenazas en Microsoft 365 está impulsada por Microsoft Intelligent Security Graph.
- Cree alertas que puedan identificar eventos maliciosos o sospechosos.
- Comprenda cómo funciona el proceso de investigación y respuesta automatizado de Microsoft 365 Defender.
- Describir cómo la búsqueda de amenazas permite a los operadores de seguridad identificar las amenazas a la ciberseguridad.
- Describa cómo la búsqueda avanzada en Microsoft 365 Defender inspecciona de forma proactiva los eventos en su red para localizar entidades e indicadores de amenazas.

Implementar la protección de aplicaciones mediante Microsoft Defender para aplicaciones en la nube

Este módulo examina cómo implementar Microsoft Defender para aplicaciones en la nube, que identifica y combate las ciberamenazas en todos sus servicios en la nube de Microsoft y de terceros.

Objetivos de aprendizaje

Al final de este módulo, usted debería ser capaz de:

- Describa cómo Microsoft Defender para aplicaciones en la nube proporciona una mejor visibilidad de la actividad de la red en la nube y aumenta la protección de los datos críticos en las aplicaciones en la nube.
- Explicar cómo implementar Microsoft Defender para aplicaciones en la nube.
- Controle sus aplicaciones en la nube con políticas de archivos.
- Administre y responda a las alertas generadas por esas políticas.
- Configurar y solucionar problemas de Cloud Discovery.

Implementación de endpoint protection mediante Microsoft Defender para punto de conexión

En este módulo se examina cómo Microsoft Defender para punto de conexión ayuda a las redes empresariales a prevenir, detectar, investigar y responder a amenazas avanzadas mediante el uso de sensores de comportamiento de puntos de conexión, análisis de seguridad en la nube e inteligencia de amenazas.

Objetivos de aprendizaje

Después de completar este módulo, debería poder:

- Microsoft Defender para punto de conexión es una plataforma concebida para ayudar a las redes empresariales a impedir, detectar e investigar amenazas avanzadas en sus puntos de conexión, y actuar ante ellas.
- Incorporar dispositivos compatibles a Microsoft Defender para punto de conexión
- Implemente el módulo administración de amenazas y vulnerabilidades para identificar, evaluar y corregir eficazmente los puntos débiles de los puntos de conexión.
- Configure la detección de dispositivos para ayudar a encontrar dispositivos no administrados conectados a la red corporativa.
- Las organizaciones pueden reducir su exposición a amenazas y vulnerabilidades corrigiendo los problemas en función de las recomendaciones de seguridad prioritarias.

Implemente la protección contra amenazas con Microsoft Defender para Office 365

Este módulo examina la pila de protección de Microsoft Defender para Office 365 y sus características de inteligencia de amenazas correspondientes, incluidos Threat Explorer, Threat Trackers y entrenamiento de simulación de ataques.

Objetivos de aprendizaje

Después de completar este módulo, debería ser capaz de:

- Describa la pila de protección proporcionada por Microsoft Defender para Office 365.
- Comprenda cómo se puede usar Threat Explorer para investigar amenazas y ayudar a proteger a su inquilino.
- Describa los widgets y las vistas de Threat Tracker que le brindan inteligencia sobre diferentes problemas de ciberseguridad que podrían afectar a su empresa.
- Ejecute escenarios de ataque realistas con el Simulador de ataques para ayudar a identificar a los usuarios vulnerables antes de que un ataque real afecte a su organización.