GADESOFT

Cybersecurity Analyst

Microsoft Solutions Partner

Microsoft Cloud Training Services

Descripción del programa

Duración: 220 horas

Objetivos

- Implementar controles de seguridad, mantener la postura de seguridad de una organización e identificar y remediar las vulnerabilidades de seguridad
- Microsoft Sentinel, Microsoft Defender para la nube y Microsoft 365 Defender
- Implementar soluciones de administración de identidades basadas en Microsoft Azure AD
- Information Protection
- Confianza cero,Cumplimiento de riesgos de gobernanza (GRC),Operaciones de seguridad (SecOps) y Microsoft Intune

Requisitos

- Conocimientos de Microsoft Azure,
- Competencias digitales básicas

Localidad: Madrid

Modalidad: Online Direct

Precio: 2.500€*

**El precio no incorpora exámenes de certificación. Los exámenes de Fundamentos 100€ y Role-Based 165€.*

Certificaciones

Security, Compliance, and Identity Fundamentals	Security Operations Analyst Associate	Identity and Access Administrator Associate
SC-900	**SC-200**	**SC-300**
Information Security Administrator Associate (beta)	Azure Security Engineer Associate	Cybersecurity Architect Expert
SC-401	**AZ-500**	**SC-100**

Contenido

Módulo 1 – Describir los conceptos de seguridad y cumplimiento

- Describir el modelo de responsabilidad compartida
- Describir la defensa en profundidad
- Describir el modelo Zero Trust
- Descripción del cifrado y el hash
- Describir los conceptos de gobernanza, riesgo y cumplimiento (GRC)

Módulo 2 – Describir los conceptos de identidad

- Definir la autenticación y la autorización
- Definir la identidad como el perímetro de seguridad principal
- Describir el rol del proveedor de identidades
- Describir el concepto de servicios de directorio y Active Directory
- Describir el concepto de federación

Módulo 3 – Describir los tipos de función e identidad de Microsoft Entra ID

- Descripción del identificador de Microsoft Entra
- Describir los tipos de identidades
- Descripción de la identidad híbrida
- Descripción de identidades externas

Módulo 4 – Descripción de las capacidades de autenticación de Microsoft Entra ID

- Describir los métodos de autenticación
- Descripción de la autenticación multifactor
- Descripción del autoservicio de restablecimiento de contraseña
- Describir las capacidades de administración y protección de contraseñas

Módulo 5 – Descripción de las capacidades de administración de acceso de Microsoft Entra

- Descripción del acceso condicional
- Descripción del acceso seguro global en Microsoft Entra
- Descripción de los roles de Microsoft Entra y el control de acceso basado en roles (RBAC)

Contenido

Módulo 6 – Describir las capacidades de protección de identidad y gobernanza de Microsoft Entra

- Descripción de la gobernanza de ID de Microsoft Entra
- Describir las revisiones de acceso
- Descripción de la administración de derechos
- Descripción de las capacidades de Privileged identity Management
- Descripción de la protección de ID de Microsoft Entra
- Descripción de la administración de permisos de Microsoft Entra
- Descripción del identificador verificado de Microsoft Entra
- Descripción de la integración de Microsoft Entra con Microsoft Copilot for Security

Módulo 7 – Descripción de Microsoft Copilot for Security

- Familiarícese con Microsoft Copilot for Security
- Descripción de la terminología de Microsoft Copilot for Security
- Describir cómo Microsoft Copilot for Security procesa las solicitudes de solicitud
- Describir los elementos de un aviso eficaz
- Descripción de cómo habilitar Microsoft Copilot for Security

Módulo 8 – Descripción de los servicios de seguridad de infraestructura principal en Azure

- Descripción de la protección DDoS de Azure
- Descripción de Azure Firewall
- Describir el firewall de aplicaciones web
- Descripción de la segmentación de red en Azure
- Descripción de los grupos de seguridad de red de Azure
- Descripción de Azure Bastion
- Descripción de Azure Key Vault

Módulo 9 – Descripción de las funcionalidades de administración de seguridad de Azure

- Definir los conceptos de SIEM y SOAR
- Descripción de las funcionalidades de detección y mitigación de amenazas en Microsoft Sentinel
- Descripción de la integración de Microsoft Sentinel con Microsoft Copilot for Security

Contenido

Módulo 10 – Descripción de la protección contra amenazas con Microsoft Defender XDR

- Descripción de los servicios XDR de Microsoft Defender
- Descripción de Microsoft Defender para Office 365
- Descripción de Microsoft Defender para punto de conexión
- Descripción de Microsoft Defender for Cloud Apps
- Descripción de Microsoft Defender for Identity
- Descripción de la administración de vulnerabilidades de Microsoft Defender
- Descripción de la inteligencia sobre amenazas de Microsoft Defender
- Descripción del portal de Microsoft Defender
- Descripción de la integración de Copilot con Microsoft Defender XDR

Módulo 11 – Describir el portal de confianza de servicios y las capacidades de privacidad de Microsoft

- Describir las ofertas del portal de confianza de servicios
- Describir los principios de privacidad de Microsoft
- Descripción de Microsoft Priva

Módulo 12 – Descripción de las soluciones de seguridad de datos de Microsoft Purview

- Describir las capacidades de clasificación de datos de Microsoft Purview Information Protection
- Descripción de etiquetas y directivas de confidencialidad en Microsoft Purview Information Protection
- Descripción de la prevención de pérdida de datos en Microsoft Purview
- Descripción de la administración de riesgos internos en Microsoft Purview
- Descripción de la protección adaptable en Microsoft Purview

Módulo 13 – Descripción de las soluciones de cumplimiento de datos de Microsoft Purview

- Descripción de la auditoría en Microsoft Purview
- Descripción de la exhibición de documentos electrónicos
- Descripción del Administrador de cumplimiento
- Describir el cumplimiento de las comunicaciones
- Describir la gestión del ciclo de vida de los datos
- Describir la administración de registros

Contenido

Módulo 14 – Descripción de las soluciones de gobernanza de datos de Microsoft Purview

- Describir los conceptos y beneficios de la gobernanza de datos
- Descripción del catálogo de datos de Microsoft Purview

Módulo 15 – Introducción a la protección contra amenazas de Microsoft Defender XDR

- Exploración de casos de uso de respuesta de Detección y respuesta extendidas (XDR)
- Descripción de Microsoft Defender XDR en un centro de operaciones de seguridad (SOC)
- Exploración de Microsoft Security Graph
- Investigación de incidentes de seguridad en Microsoft Defender XDR

Módulo 16 – Mitigación de incidentes con Microsoft 365 Defender

- Uso del portal de Microsoft Defender
- Administración de incidentes
- Investigación de incidentes
- Administración e investigación de alertas
- Administración de investigaciones automatizadas
- Utilice el centro de actividades
- Exploración de la búsqueda avanzada
- Investigación de los registros de inicio de sesión de Microsoft Entra
- Información sobre la puntuación segura de Microsoft
- Análisis de amenazas
- Análisis de los informes
- Configuración del portal de Microsoft Defender

Módulo 17 – Corrección de riesgos con Microsoft Defender para Office 365

- Automatizar, investigar y remediar
- Configurar, proteger y detectar
- Simular ataques

Contenido

Módulo 18 – Administrar Microsoft Entra Identity Protection

- Revisión de los conceptos básicos de Identity Protection
- Implementación y administración de directivas de riesgo de usuario
- Ejercicio: Habilitación de una directiva de riesgo de inicio de sesión
- Ejercicio para configurar la directiva de registro de autenticación multifactor de Microsoft Entra
- Supervisar, investigar y solucionar los problemas con los usuarios de riesgo elevado
- Implementación de la seguridad para las identidades de carga de trabajo
- Explorar Microsoft Defender for Identity

Módulo 19 – Protección del entorno con Microsoft Defender for Identity

- Configurar sensores de Microsoft Defender for Identity
- Revisar las cuentas o datos comprometidos
- Integrar con otras herramientas de Microsoft

Módulo 20 – Protección de aplicaciones y servicios en la nube con Microsoft Defender for Cloud Apps

- Definir el marco de Defender for Cloud Apps
- Explorar sus aplicaciones en la nube con Cloud Discovery
- Proteger los datos y aplicaciones con el control de aplicaciones de acceso condicional
- Clasificar y proteger información confidencial
- Detectar amenazas

Módulo 21 – Aspectos básicos de la IA generativa

- ¿Qué es la inteligencia artificial generativa?
- ¿Qué son los modelos de lenguaje?
- Uso de modelos de lenguaje
- ¿Qué son los copilotos?
- Microsoft Copilot
- Consideraciones para los mensajes de Copilot
- Extensión y desarrollo de copilotos
- Ejercicio: Exploración de Microsoft Copilot

Contenido

Módulo 22 – Descripción de Seguridad de Microsoft Copilot

- Familiarícese con Microsoft Security Copilot
- Descripción de la terminología de Seguridad de Microsoft Copilot
- Descripción de cómo Microsoft Security Copilot procesa solicitudes de avisos
- Describir los elementos de un mensaje eficaz
- Descripción de cómo habilitar Microsoft Security Copilot

Módulo 23 – Descripción de las características principales de Seguridad de Microsoft Copilot

- Descripción de las características disponibles en la experiencia independiente de Seguridad de Microsoft Copilot
- Describir las características disponibles en una sesión de la experiencia independiente
- Descripción de los complementos de Microsoft disponibles en Microsoft Security Copilot
- Describir los complementos ajenos a Microsoft compatibles con Microsoft Security Copilot
- Descripción de los libros de solicitudes personalizados
- Descripción de las conexiones de la base de conocimiento

Módulo 24 – Descripción de experiencias integradas de Seguridad de Microsoft Copilot

- Describir Copilot en Microsoft Defender XDR
- Copilot en Microsoft Purview
- Copilot en Microsoft Entra
- Copilot en Microsoft Intune
- Copilot en Microsoft Defender for Cloud (versión preliminar)

Módulo 25 – Exploración de casos de uso de Seguridad de Microsoft Copilot

- Explorar la experiencia de primera ejecución
- Exploración de la experiencia independiente
- Configuración del complemento de Microsoft Sentinel
- Habilitar un complemento personalizado
- Exploración de las cargas de archivos como una base de conocimiento
- Crear una secuencia de indicaciones personalizada
- Exploración de las funcionalidades de Copilot en XDR de Microsoft Defender
- Explorar las funcionalidades de Copilot en Microsoft Purview

Contenido

Módulo 26 – Respuesta a las alertas de prevención de pérdida de datos mediante Microsoft 365

- Describir las alertas de prevención de pérdida de datos
- Investigación de las alertas de prevención de pérdida de datos en Microsoft Purview
- Investigación de alertas de prevención de pérdida de datos en Microsoft Defender for Cloud Apps

Módulo 27 – Administración del riesgo interno en Microsoft Purview

- Información general sobre la administración de riesgos internos
- Introducción a la administración de directivas de riesgo interno
- Creación y administración de directivas de riesgo interno
- Investigación de alertas de riesgo interno
- Tomar medidas sobre las alertas de riesgo interno a través de los casos
- Gestione las pruebas forenses de la gestión de riesgos internos
- Creación de plantillas de aviso de administración de riesgos internos

Módulo 28 – Búsqueda e investigación con la auditoría de Microsoft Purview

- Introducción a Auditoría de Microsoft Purview
- Configuración y administración de Auditoría de Microsoft Purview
- Realización de búsquedas con Auditoría (Estándar)
- Auditar interacciones de Microsoft Copilot para Microsoft 365
- Investigar actividades con Auditoría (Premium)
- Exportar datos de registro de auditoría
- Configuración de la retención de auditoría con Auditoría (Premium)

Módulo 29 – Investigación de amenazas con búsqueda de contenido en Microsoft Purview

- Soluciones de exhibición de documentos electrónicos de Microsoft Purview
- Crear una búsqueda de contenido
- Ver los resultados y las estadísticas de la búsqueda
- Exportar los resultados de búsqueda y el informe de búsqueda
- Configurar el filtrado de permisos de búsqueda
- Buscar y eliminar mensajes de correo electrónico

Contenido

Módulo 30 – Protección contra amenazas con Microsoft Defender para punto de conexión

- Practicar la administración de seguridad
- Buscar amenazas dentro de su red

Módulo 31 – Implementación del entorno de Microsoft Defender para punto de conexión

- Creación del entorno
- Descripción de la compatibilidad y las características de los sistemas operativos
- Incorporación de dispositivos
- Administración del acceso
- Creación y administración de roles para el control de acceso basado en roles
- Configuración de los grupos de dispositivos
- Configuración de las características avanzadas del entorno

Módulo 32 – Implementación de mejoras de seguridad de Windows con Microsoft Defender para punto de conexión

- Descripción de la reducción de la superficie expuesta a ataques
- Habilitar reglas de reducción de la superficie expuesta a ataques

Módulo 33 – Realización de investigaciones de dispositivos en Microsoft Defender para punto de conexión

- Uso de la lista de inventario de dispositivos
- Investigación del dispositivo
- Uso del bloqueo de comportamiento
- Detección de dispositivos con detección de dispositivos

Módulo 34 – Realizar acciones en un dispositivo con Microsoft Defender para punto de conexión

- Explicación de las acciones del dispositivo
- Ejecución del examen de Antivirus de Microsoft Defender en los dispositivos
- Recopilación del paquete de investigación desde los dispositivos
- Inicio de una sesión de respuesta dinámica

Contenido

Módulo 35 – Llevar a cabo investigaciones sobre evidencias y entidades con Microsoft Defender para punto de conexión

- Investigar un archivo
- Investigación de una cuenta de usuario
- Investigar una dirección IP
- Investigar un dominio

Módulo 36 – Configuración y administración de la automatización con Microsoft Defender para punto de conexión

- Configurar características avanzadas
- Administración de la configuración de carga y carpeta de automatización
- Configuración de las capacidades de investigación y corrección automatizadas
- Bloqueo de dispositivos en riesgo

Módulo 37 – Configuración de alertas y detecciones en Microsoft Defender para punto de conexión

- Configurar características avanzadas
- Configurar notificaciones de alerta
- Administración de la eliminación de alertas
- Administración de los indicadores

Módulo 38 – Uso de administración de vulnerabilidades en Microsoft Defender para punto de conexión

- Descripción de Administración de amenazas y vulnerabilidades
- Exploración de las vulnerabilidades de sus dispositivos
- Administración de la corrección

Módulo 39 – Explicación de las protecciones de las cargas de trabajo en la nube en Microsoft Defender para la nube

- Explicación de Microsoft Defender para la nube
- EDescripción de la protección de cargas de trabajo de Microsoft Defender para la nube
- Ejercicio: Guía interactiva de Microsoft Defender para la nube
- Habilitar Microsoft Defender for Cloud

Contenido

Módulo 40 – Conexión de recursos de Azure a Microsoft Defender para la nube

- Exploración y administración de los recursos con Asset Inventory
- Configuración del aprovisionamiento automático
- Aprovisionamiento manual del agente de log Analytics

Módulo 41 – Conexión de recursos que no son de Azure a Microsoft Defender for Cloud

- Protección de recursos que no son de Azure
- Conexión de máquinas que no son de Azure
- Conexión de cuentas de AWS
- Conexión de cuentas de GCP

Módulo 42 – Administración de la posición de seguridad en la nube

- Exploración de la puntuación de seguridad
- Explorar recomendaciones
- Medición y aplicación del cumplimiento normativo
- Descripción de Workbooks

Módulo 43 – Explicación de las protecciones de las cargas de trabajo en la nube en Microsoft Defender for Cloud

- Información sobre Microsoft Defender para servidores
- Información sobre Microsoft Defender para Storage
- Información sobre Microsoft Defender para SQL
- Información sobre Microsoft Defender para bases de datos de código abierto
- Información sobre Microsoft Defender para Key Vault
- Información sobre Microsoft Defender para Resource Manager
- Información sobre Microsoft Defender para DNS
- Descripción de Microsoft Defender para contenedores
- Información sobre las protecciones adicionales de Microsoft Defender

Contenido

Módulo 44 – Correción de alertas de seguridad mediante Microsoft Defender for Cloud

- Descripción de las alertas de seguridad
- Corrección de alertas y automatización de respuestas
- Supresión de alertas de Defender for Cloud
- Generación de informes de inteligencia sobre amenazas
- Respuesta a alertas desde recursos de Azure

Módulo 45 – Construcción de instrucciones KQL para Microsoft Sentinel

- Descripción de la estructura de instrucciones del lenguaje de consulta Kusto
- Uso del operador de búsqueda
- Uso del operador where
- Uso de la instrucción Let
- Uso del operador extend
- Uso del operador order by
- Uso de los operadores project

Módulo 46 – Uso de KQL para analizar los resultados de consultas

- Uso del operador summarize
- Uso del operador summarize para filtrar resultados
- Uso del operador summarize para preparar los datos
- Uso del operador render para crear visualizaciones

Módulo 47 – Uso de KQL para crear instrucciones de varias tablas

- Uso del operador union
- Uso del operador join

Módulo 48 – Trabajo con datos en Microsoft Sentinel mediante el lenguaje de consulta Kusto

- Extracción de datos de campos de cadena no estructurados
- Extracción de datos de datos de cadena estructurados
- Integración de datos externos
- Creación de analizadores con funciones

Contenido

Módulo 49 – Introducción a Microsoft Sentinel

- ¿Qué es Microsoft Sentinel?
- Funcionamiento de Microsoft Sentinel
- Cuándo usar Microsoft Sentinel

Módulo 50 – Creación y administración de áreas de trabajo de Microsoft Sentinel

- Plan para el área de trabajo de Microsoft Sentinel
- Creación de un área de trabajo de Microsoft Sentinel
- Administración de áreas de trabajo en los inquilinos mediante Azure Lighthouse
- Información sobre los permisos y roles de Microsoft Sentinel
- Administración de la configuración de Microsoft Sentinel
- Configuración de registros

Módulo 51 – Registros de consulta en Microsoft Sentinel

- Consulta de registros en la página de registros
- Información sobre las tablas de Microsoft Sentinel
- Descripción de las tablas comunes
- Descripción de las tablas de Microsoft Defender XDR

Módulo 52 – Uso de listas de reproducción en Microsoft Sentinel

- Planear listas de reproducción
- Creación de una lista de reproducción
- Administración de listas de reproducción

Módulo 53 – Uso de la inteligencia sobre amenazas en Microsoft Sentinel

- Definición de Inteligencia sobre amenazas
- Definición de Inteligencia sobre amenazas
- Administrar los indicadores de amenazas
- Visualización de los indicadores de amenazas con KQL

Contenido

Módulo 54 – Integración de Microsoft Denfender XDR con Microsoft Sentinel

- Comprender los beneficios de integrar Microsoft Sentinel con Defender XDR
- Explorar las diferencias de capacidades entre los portales de Microsoft Defender XDR y Microsoft Sentinel
- Incorporación de Microsoft Sentinel a Microsoft Defender XDR
- Explorar las características de Microsoft Sentinel en Microsoft Defender XDR

Módulo 55 – Conexión de datos a Microsoft Sentinel mediante conectores de datos

- Ingesta de datos de registro con conectores de datos
- Descripción de los proveedores de conectores de datos
- Visualización de hosts conectados

Módulo 56 – Conexión de servicios Microsoft a Microsoft Sentinel

- Planeamiento para usar conectores de servicios de Microsoft
- Conexión del conector de Microsoft Office 365
- Conectar el conector de Microsoft Entra
- Conectar el conector de protección de Microsoft Entra ID
- Conexión del conector de actividad de Azure

Módulo 57 – Conexión de Microsoft Defender XDR a Microsoft Sentinel

- Planear conectores de Microsoft Defender XDR
- Conexión del conector de Microsoft Defender XDR
- Conexión del conector de Microsoft Defender for Cloud
- Conexión de Microsoft Defender para IoT
- Conexión de los conectores heredados de Microsoft Defender

Módulo 58 – Conexión de hosts de Windows a Microsoft Sentinel

- Planeamiento para usar el conector de eventos de seguridad de hosts Windows
- Conexión mediante eventos de seguridad de Windows a través del conector AMA
- Conexión mediante eventos de seguridad a través del conector del agente antiguo
- Recopilación de registros de eventos de Sysmon

Contenido

Módulo 59 – Conexión de registros de formato de evento común a Microsoft Sentinel

- Planeamiento para usar el conector de formato de evento común
- Conexión de una solución externa mediante el conector de formato de evento común

Módulo 60 – Conexión de orígenes de datos Syslog a Microsoft Sentinel

- Planeamiento de la recopilación de datos de Syslog
- Recopilación de datos de orígenes basados en Linux mediante Syslog
- Configuración de la regla de recopilación de datos para orígenes de datos de Syslog
- Análisis de los datos de syslog con KQL

Módulo 61 – Conexión de indicadores de amenazas a Microsoft Sentinel

- Planeamiento para usar conectores de inteligencia sobre amenazas
- Conexión del conector TAXII de inteligencia sobre amenazas
- Conexión del conector de plataformas de inteligencia sobre amenazas
- Visualización de los indicadores de amenazas con KQL

Módulo 62 – Detección de amenazas con análisis de Microsoft Sentinel

- Ejercicio: Detección de amenazas con análisis de Microsoft Sentinel
- ¿Qué es Análisis de Microsoft Sentinel?
- Tipos de reglas de análisis
- Creación de una regla de análisis a partir de plantillas
- Creación de una regla de análisis a partir del asistente
- Administración de reglas de análisis
- Ejercicio: Detección de amenazas con análisis de Microsoft Sentinel

Módulo 63 – Automatización en Microsoft Sentinel

- Descripción de las opciones de automatización
- Creación de reglas de automatización

Contenido

Módulo 64 – Respuesta a amenazas con cuadernos de estrategias de Microsoft Sentinel

- Ejercicio: Creación de un cuaderno de estrategias de Microsoft Sentinel
- ¿Qué son los cuadernos de estrategias de Microsoft Sentinel?
- Desencadenamiento de un cuaderno de estrategias en tiempo real
- Ejecución de cuadernos de estrategias a petición
- Ejercicio: Creación de un cuaderno de estrategias de Microsoft Sentinel

Módulo 65 – Administración de incidentes de seguridad en Microsoft Sentinel

- Ejercicio: Configuración del entorno de Azure
- Descripción de incidentes
- Evidencia y entidades de un incidente
- Administración de incidentes
- Ejercicio: Investigación de un incidente

Módulo 66 – Identificación de amenazas con análisis de comportamiento

- Descripción del análisis de comportamiento
- Exploración de entidades
- Visualización de información de comportamiento de entidades
- Uso de plantillas de reglas analíticas de detección de anomalías

Módulo 67 – Normalización de datos en Microsoft Sentinel

- Descripción de la normalización de datos
- Uso de analizadores de ASIM
- Descripción de las funciones KQL parametrizadas
- Creación de un analizador de ASIM
- Configuración de reglas de recopilación de datos de Azure Monitor

Contenido

Módulo 68 – Consulta, visualización y supervisión de datos en Microsoft Sentinel

- Ejercicio: Consulta y visualización de datos con libros de Microsoft Sentinel
- Supervisión y visualización de datos
- Consulta de datos mediante el lenguaje de consulta Kusto
- Uso de libros predeterminados de Microsoft Sentinel
- Creación de un libro de Microsoft Sentinel
- Ejercicio: Visualización de datos mediante libros de Microsoft Sentinel

Módulo 69 – Administración de contenido en Microsoft Sentinel

- Uso de soluciones desde el centro de contenido
- Uso de repositorios para la implementación

Módulo 70 – Explicación de los conceptos de búsqueda de amenazas en Microsoft Sentinel

- Concepto de búsqueda de amenazas de ciberseguridad
- Desarrollo de una hipótesis
- Explorar MITRE ATT&CK

Módulo 71 – Búsqueda de amenazas con Microsoft Sentinel

- Configuración del ejercicio
- Exploración de la creación y administración de consultas de búsqueda de amenazas
- Conservación de hallazgos importantes con marcadores
- Observación de amenazas a lo largo del tiempo con streaming en vivo
- Ejercicio: Búsqueda de amenazas mediante Microsoft Sentinel

Módulo 72 – Uso de trabajos de búsqueda en Microsoft Sentinel

- Búsqueda con un trabajo de búsqueda
- Restauración de datos históricos

Módulo 73 – Búsqueda de amenazas con cuadernos en Microsoft Sentinel

- Acceso a los datos de Azure Sentinel con herramientas externas
- Búsqueda con cuadernos
- Creación de un cuaderno
- Exploración del código del cuaderno

Contenido

Módulo 74 – Exploración de identidades en Microsoft Entra ID

- Explicación del panorama de identidades
- Exploración de confianza cero con identidad
- Debate sobre la identidad como un plano de control
- Exploración de por qué tenemos identidad
- Definición de la administración de identidades
- Contraste de la identidad descentralizada con sistemas de identidad central
- Debate sobre soluciones de administración de identidades
- Explicación de Microsoft Entra negocio a negocio
- Comparación de proveedores de identidades de Microsoft
- Definición de licencias de identidad
- Exploración de la autenticación
- Debate sobre la autorización
- Explicación de la auditoría en la identidad

Módulo 75 – Implementación de la configuración inicial de Microsoft Entra ID

- Configuración de la marca de empresa
- Configuración y administración de roles de Microsoft Entra
- Ejercicio de administración de roles de usuarios
- Configuración de la delegación mediante unidades administrativas
- Analizar permisos de rol de Microsoft Entra
- Configuración y administración de dominios personalizados
- Configuración para todo el inquilino
- Ejercicio: configuración de propiedades para todo el inquilino

Módulo 76 – Crear, configurar y administrar identidades

- Crear, configurar y administrar usuarios.
- Ejercicio: Asignar licencias a usuarios
- Ejercicio: Restaurar o quitar usuarios eliminados
- Crear, configurar y administrar grupos.
- Ejercicio: Adición de grupos en Microsoft Entra ID
- Configuración y administración del registro de dispositivos
- Administrar licencias
- Ejercicio: Cambiar las asignaciones de licencias de grupo
- Ejercicio: Cambiar las asignaciones de licencias de usuario
- Creación de atributos de seguridad personalizados
- Exploración de la creación automática de usuarios

Contenido

Módulo 77 – Implementación y administración de identidades externas

- Descripción del acceso de invitado y las cuentas de negocio a negocio
- Administración de la colaboración externa
- Ejercicio: Configurar la colaboración externa
- Invitación a usuarios externos, de forma individual y masiva
- Ejercicio: Agregar usuarios invitados a un directorio
- Ejercicio: Invitar a usuarios invitados de forma masiva
- Demostración: administración de usuarios invitados en Microsoft Entra ID
- Administración de cuentas de usuario externas en Microsoft Entra ID
- Administración de usuarios externos en cargas de trabajo de Microsoft 365
- Ejercicio: Explorar los grupos dinámicos
- Implementación y administración de Microsoft Entra Verified ID
- Configuración de proveedores de identidades
- Implementación de controles de acceso entre inquilinos

Módulo 78 – Implementación y administración de una identidad híbrida

- Planear, diseñar e implementar Microsoft Entra Connect
- Implementación y administración de la sincronización de hash de contraseña (PHS)
- Implementación y administración de la autenticación de tránsito (PTA)
- Demostración: Administración de la autenticación transferida y el inicio de sesión único (SSO) de conexión directa
- Implementación y administración de la federación
- Solución de errores de sincronización
- Implementación de Microsoft Entra Connect Health
- Administrar Microsoft Entra Health

Módulo 79 – Protección de usuarios de Microsoft Entra con autenticación multifactor

- ¿Qué es la autenticación multifactor de Microsoft Entra?
- Planificación de la implementación de la autenticación multifactor
- Ejercicio: Habilitación de la autenticación multifactor de Microsoft Entra
- Configuración de métodos de autenticación multifactor

Contenido

Módulo 80 – Administrar la autenticación de usuarios

- Administrar FIDO2 y métodos de autenticación sin contraseña
- Exploración de la aplicación Authenticator y tokens de OATH
- Implementar una solución de autenticación basada en Windows Hello para empresas
- Ejercicio: Configurar e implementar el autoservicio de restablecimiento de contraseña
- Implementación y administración de la protección de contraseñas
- Configuración de umbrales de bloqueo inteligente
- Ejercicio: Administración de valores de bloqueo inteligente de Microsoft Entra
- Implementación de Kerberos y autenticación basada en certificados en Microsoft Entra ID
- Configuración de la autenticación de usuarios de Microsoft Entra para máquinas virtuales

Módulo 81 – Planificación, implementación y administración del acceso condicional

- Planificación de los valores predeterminados de seguridad
- Ejercicio: Uso de los valores predeterminados de seguridad
- Planificación de directivas de acceso condicional
- Implementación de controles y asignaciones de directivas de acceso condicional
- Ejercicio: Implementación de roles y asignaciones de directivas de acceso condicional
- Prueba de las directivas de acceso condicional y solución de problemas relacionados
- Implementación de controles de aplicación
- Implementación de la administración de sesiones
- Ejercicio: Configuración de los controles de sesión de autenticación
- Implementación de la evaluación continua de acceso

Módulo 82 – Administrar Microsoft Entra Identity Protection

- Revisión de los conceptos básicos de Identity Protection
- Implementación y administración de directivas de riesgo de usuario
- Ejercicio: Habilitación de una directiva de riesgo de inicio de sesión
- Ejercicio para configurar la directiva de registro de autenticación multifactor de Microsoft Entra
- Supervisar, investigar y solucionar los problemas con los usuarios de riesgo elevado
- Implementación de la seguridad para las identidades de carga de trabajo
- Explorar Microsoft Defender for Identity

Contenido

Módulo 83 – Implementación de la administración del acceso para recursos de Azure

- Asignación de roles de Azure
- Configuración de roles personalizados de Azure
- Creación y configuración de identidades administradas
- Acceso a recursos de Azure con identidades administradas
- Análisis de permisos de rol de Azure
- Configuración de directivas de RBAC de Azure Key Vault
- Recuperación de objetos de Azure Key Vault
- Explorar la Administración de permisos de Microsoft Entra

Módulo 84 – Implementación y configuración de acceso global seguro de Microsoft Entra

- Exploración del acceso seguro global
- Implementación y configuración de Acceso a Internet de Microsoft Entra
- Implementación y configuración de Acceso privado de Microsoft Entra
- Exploración del uso del panel para impulsar el acceso seguro global
- Creación de redes remotas para su uso con Acceso global seguro
- Uso del acceso condicional con Acceso global seguro
- Exploración de registros y opciones de supervisión con Acceso global seguro

Módulo 85 – Planeación y diseño de la integración de aplicaciones empresariales para SSO

- Descubrimiento de aplicaciones mediante Microsoft Defender for Cloud Apps y el informe de aplicaciones de Servicios de federación de Active Directory (AD FS)
- Configuración de conectores en aplicaciones
- Ejercicio: Implementación de la administración de acceso para aplicaciones
- Diseño e implementación de roles de administración de aplicaciones
- Ejercicio: Creación de un rol personalizado para administrar el registro de aplicaciones
- Configuración de aplicaciones SaaS preintegradas de la galería
- Implementación y administración de directivas para aplicaciones de OAuth

Contenido

Módulo 86 – Implementación y supervisión de la integración de aplicaciones empresariales para el inicio de sesión único

- Implementar personalizaciones de tokens
- Implementación y configuración de las opciones de consentimiento
- Integrar las aplicaciones locales con Application Proxy de Microsoft Entra
- Integración de aplicaciones SaaS personalizadas para el inicio de sesión único
- Implementación del aprovisionamiento de usuarios basado en aplicaciones
- Supervisar y auditar el acceso a las aplicaciones empresariales integradas en Microsoft Entra
- Creación y administración de colecciones de aplicaciones

Módulo 87 – Implementación del registro de aplicaciones

- Planear la estrategia de registro de la aplicación de línea de negocio
- Implementación de registros de aplicaciones
- Registro de una aplicación
- Configuración del permiso para una aplicación
- Concesión del consentimiento del administrador para todo el inquilino a aplicaciones
- Implementación de la autorización de la aplicación
- Ejercicio para añadir roles de aplicación a una aplicación y recibir tokens
- Administración y supervisión de aplicaciones mediante la gobernanza de aplicaciones

Módulo 88 – Registro de aplicaciones con Microsoft Entra ID

- Planeamiento para el registro de aplicaciones
- Exploración de objetos de aplicación y entidades de servicio
- Crear registros de aplicaciones
- Configuración de la autenticación de aplicaciones
- Configurar permisos de API
- Creación de roles de aplicación

Módulo 89 – Planificación e implementación de la administración de derechos

- Definición de los paquetes de acceso
- Ejercicio: creación y administración de un catálogo de recursos con la administración de derechos de Microsoft Entra
- Configuración de la administración de derechos
- Ejercicio: adición del informe de aceptación de los términos de uso
- Ejercicio: administración del ciclo de vida de los usuarios externos con la gobernanza de identidades de Microsoft Entra
- Configuración y administración de organizaciones conectadas
- Revisión de derechos por usuario

Contenido

Módulo 90 – Planteamiento, implementación y administración de la revisión de acceso

- Planear revisiones de acceso
- Crear revisiones de acceso para grupos y aplicaciones
- Creación y configuración de programas de revisión de acceso
- Supervisar los resultados de la revisión de acceso
- Automatizar las tareas de administración de revisiones de acceso
- Configurar revisiones de acceso periódicas

Módulo 91 – Planificación e implementación de acceso con privilegios

- Definición de una estrategia de acceso con privilegios para usuarios administrativos
- Configurar Privileged Identity Management para recursos de Azure
- Ejercicio de configuración de Privileged Identity Management para roles de Microsoft Entra
- Ejercicio para asignar roles de Microsoft Entra en Privileged Identity Management
- Ejercicio: asignación de roles de recursos de Azure en Privileged Identity Management
- Planeamiento y configuración de grupos de acceso con privilegios
- Análisis del historial de auditoría e informes de Privileged Identity Management
- Crear y administrar cuentas de acceso de emergencia

Módulo 92 – Supervisión y mantenimiento de Microsoft Entra ID

- Análisis e investigación de los registros de inicio de sesión para solucionar problemas de acceso
- Revisión y supervisión de los registros de auditoría de Microsoft Entra
- Ejercicio: conexión de datos de Microsoft Entra ID a Microsoft Sentinel
- Exportación de registros a la información de seguridad de terceros y al sistema de administración de eventos
- Análisis de libros e informes de Microsoft Entra
- Supervisión de la posición de seguridad con la puntuación de seguridad de la identidad

Contenido

Módulo 93 – Explorar las muchas características de administración de permisos de Microsoft Entra

- Una experiencia completa para todos los entornos en la nube
- Obtención de información de nivel general en el panel Administración de permisos
- Comprobación de conocimientos: Conclusiones
- Profundización en la pestaña Análisis
- Comprobación de conocimientos: Análisis
- Desarrollar una mejor comprensión de su entorno con informes
- Análisis de datos históricos con la pestaña Auditoría
- Actuar sobre los resultados con la pestaña Corrección de administración de permisos
- Comprobación de conocimientos: Corrección
- Adoptar un enfoque más proactivo para la administración con supervisión continua
- Comprobación de conocimientos: Supervisión
- Administración del acceso a la Administración de permisos de Microsoft Entra

Módulo 94 – Implementación de Microsoft Purview Information Protection

- Protección de datos confidenciales en un mundo digital
- Clasificación de datos para protección y gobernanza
- Revisión y análisis de la clasificación y protección de datos
- Creación y administración de tipos de información confidencial
- Creación y configuración de etiquetas de confidencialidad con Microsoft Purview
- Aplicación de etiquetas de confidencialidad para la protección de datos
- Clasificación y protección de datos locales con Microsoft Purview
- Descripción del cifrado de Microsoft 365
- Protección del correo electrónico con el cifrado de mensajes de Microsoft Purview

Módulo 95 – Implementación y administración de la prevención de pérdida de datos de Microsoft Purview

- Evitar la pérdida de datos en Microsoft Purview
- Implementación de la prevención de pérdida de datos (DLP) en punto de conexión con Microsoft Purview
- Configuración de directivas DLP para Microsoft Defender for Cloud Apps y Power Platform
- Investigar y responder a alertas de prevención de pérdida de datos de Microsoft Purview

Contenido

Módulo 96 – Implementación y administración de Administración de riesgos internos de Microsoft Purview

- Comprender la Administración de riesgos internos de Microsoft Purview
- Preparación para la administración de riesgos internos de Microsoft Purview
- Creación y administración de directivas de administración de riesgos internos
- Investigación de alertas de riesgo interno y actividad relacionada
- Implementación de la protección adaptable en Insider Risk Management

Módulo 97 – Protección de Datos en Aplicaciones de AI con Microsoft Purview

- Descubrir las interacciones de la IA con Microsoft Purview
- Proteger los datos confidenciales frente a riesgos relacionados con la IA
- Gobernar el uso de la IA con Microsoft Purview
- Evaluar y mitigar los riesgos de la IA con Microsoft Purview

Módulo 98 – Implementación y administración de la retención y recuperación de Microsoft 365

- Comprender la retención en Microsoft Purview
- Implementación y administración de la retención y recuperación de Microsoft 365

Módulo 99 – Actividad de auditoría y búsqueda en Microsoft Purview

- Búsqueda e investigación con Microsoft Purview Audit
- Buscar contenido con eDiscovery de Microsoft Purview

Contenido

Módulo 100 – Administración de controles de seguridad para la identidad y el acceso

- Microsoft Cloud Security Benchmark: Gestión de identidades y acceso privilegiado
- ¿Qué es Microsoft Entra ID?
- Asegurar usuarios de Microsoft Entra
- Crear un nuevo usuario en Microsoft Entra ID
- Asegurar grupos de Microsoft Entra
- Recomendar cuándo usar identidades externas
- Asegurar identidades externas
- Implementar Microsoft Entra Identity Protection
- Microsoft Entra Connect
- Microsoft Entra Cloud Sync
- Opciones de autenticación
- Sincronización de hash de contraseñas con Microsoft Entra ID
- Autenticación de paso a través de Microsoft Entra
- Federación con Microsoft Entra ID
- ¿Qué es la autenticación de Microsoft Entra?
- Implementar autenticación multifactor (MFA)
- Autenticación Kerberos
- New Technology Local Area Network Manager (NTLM)
- Opciones de autenticación sin contraseña para Microsoft Entra ID
- Implementar autenticación sin contraseña
- Implementar protección de contraseñas
- Inicio de sesión único de Microsoft Entra ID
- Implementar inicio de sesión único (SSO)
- Integrar inicio de sesión único (SSO) y proveedores de identidad
- Introducción a Microsoft Entra Verified ID
- Configurar Microsoft Entra Verified ID
- Recomendar y hacer cumplir protocolos de autenticación modernos
- Grupos de administración de Azure
- Configurar permisos de roles de Azure para grupos de administración, suscripciones, grupos de recursos y recursos
- Control de acceso basado en roles de Azure
- Roles integrados de Azure
- Asignar permisos de roles de Azure para grupos de administración, suscripciones, grupos de recursos y recursos
- Roles integrados de Microsoft Entra
- Asignar roles integrados en Microsoft Entra ID
- Control de acceso basado en roles de Microsoft Entra
- Crear y asignar un rol personalizado en Microsoft Entra ID
- Gestión de permisos de Microsoft Entra
- Implementar y administrar la gestión de permisos de Microsoft Entra

Contenido

- Seguridad Zero Trust
- Microsoft Entra Privileged Identity Management
- Configurar Privileged Identity Management
- Gobernanza de Microsoft Entra ID
- Gestión del ciclo de vida de identidades
- Flujos de trabajo del ciclo de vida
- Gestión de derechos
- Delegación y roles en la gestión de derechos
- Revisiones de acceso
- Configurar gestión de roles y revisiones de acceso mediante la gobernanza de Microsoft Entra ID
- Implementar políticas de acceso condicional

Módulo 101 – Administrar el acceso a aplicaciones en el identificador de Microsoft Entra

- Administrar el acceso a las aplicaciones empresariales en Microsoft Entra ID, incluidas las concesiones de permisos de OAuth
- Administración de registros de aplicaciones en Microsoft Entra ID
- Configuración de los ámbitos del permiso de registro de aplicaciones
- Administración del consentimiento de permisos del registro de aplicaciones
- Administración y uso de entidades de servicio
- Administración de identidades administradas para recursos de Azure
- Recomendación sobre cuándo usar y configurar una instancia de Microsoft Entra Application Proxy, incluida la autenticación

Módulo 102 – Planificación e implementación de seguridad de redes virtuales

- ¿Qué es una red virtual de Azure?
- Planificación e implementación de grupos de seguridad de red (NSG) y grupos de seguridad de aplicaciones (ASG)
- Planeación e implementación de rutas definidas por el usuario (UDR)
- Planeación e implementación del emparejamiento de red virtual o puerta de enlace
- Planeación e implementación de Virtual Wide Area Network, incluyendo el centro virtual protegido
- Protección de la conectividad VPN, incluido el punto a sitio y el sitio a sitio
- Azure ExpressRoute
- Implementar el cifrado en ExpressRoute
- Configuración del firewall en recursos de PaaS
- Supervisión de la seguridad de red mediante Network Watcher, incluidos los grupos de seguridad de red

Contenido

Módulo 103– Planificación e implementación de seguridad del acceso privado a recursos de Azure

- Planeamiento e implementación de puntos de conexión de servicio de red virtual
- Planeamiento e implementación de puntos de conexión privados
- Planeamiento e implementación de servicios de Private Link
- Planeamiento e implementación de la integración de red de Azure App Service y Azure Functions
- Planeamiento e implementación de configuraciones de seguridad de red de una instancia de App Service Environment (ASE)
- Planeamiento e implementación de configuraciones de seguridad de red de una instancia de Azure SQL Managed Instance

Módulo 104 – Planificación e implementación de seguridad del acceso público a recursos de Azure

- Planee e implemente la seguridad de la capa de transporte (TLS) en las aplicaciones, incluido Azure App Service y API Management
- Planificación, implementación y administración de una instancia de Azure Firewall, las directivas de firewall y Azure Firewall Manager
- Planeamiento e implementación de una instancia de Azure Application Gateway
- Planear e implementar un firewall de aplicaciones web (WAF)
- Planeamiento e implementación de una instancia de Azure Front Door, incluido Content Delivery Network (CDN)
- Se recomienda cuándo usar Azure DDoS Protection Standard

Módulo 105 – Planificación e implementación de seguridad avanzada de procesos

- Planee e implemente el acceso remoto a puntos de conexión públicos, Azure Bastion y el acceso a una máquina virtual (VM) cuando sea necesario (JIT)
- ¿Qué es Azure Kubernetes Service?
- Configurar el aislamiento de redes en Azure Kubernetes Service (AKS)
- Protección y supervisión de Azure Kubernetes Service
- Configuración de la autenticación para Azure Kubernetes Service
- Configure la seguridad para Azure Container Instances (ACI)
- Configure la seguridad de Azure Container Apps (ACA)
- Administrar el acceso a Azure Container Registry (ACR)
- Configure el cifrado de disco, Azure Disk Encryption (ADE), el cifrado como host y el cifrado de disco confidencial
- Recomendar configuraciones de seguridad para Azure API Management

Contenido

Módulo 106 – Planificación e implementación de seguridad de almacenamiento

- Almacenamiento de Azure
- Configuración del control de acceso para las cuentas de almacenamiento
- Administración del ciclo de vida de las claves de acceso de la cuenta de almacenamiento
- Selección y configuración de un método adecuado para el acceso a Azure Files
- Selección y configuración de un método adecuado para acceder a blobs de Azure
- Selección y configuración de un método adecuado para acceder a Azure Tables
- Seleccionar y configurar un método adecuado para acceder a Azure Queues
- Seleccionar y configurar los métodos adecuados para proteger de amenazas de seguridad de datos, incluidas las eliminaciones temporales, las copias de seguridad, el control de versiones y el almacenamiento inmutable
- Configuración de Bring Your Own Key (BYOK)
- Habilitación del cifrado doble en el nivel de infraestructura de Azure Storage

Módulo 107 – Planificación e implementación de seguridad de Azure SQL Database y Azure SQL Managed Instance

- Seguridad de Azure SQL Database y de SQL Managed Instance
- Habilitación de la autenticación de base de datos mediante Microsoft Entra ID
- Habilitación y supervisión de la auditoría de bases de datos
- Identificar casos de uso del Portal de gobernanza de Microsoft Purview
- Implementar la clasificación de datos de información confidencial con el Portal de gobernanza de Microsoft Purview
- Planeamiento e implementación de enmascaramiento dinámico
- Implementar cifrado de datos transparente
- Recomendar cuándo usar Always Encrypted de Azure SQL Database

Módulo 108 – Implementación y administración del cumplimiento de las directivas de gobernanza en la nube

- Microsoft Cloud Security Benchmark: Acceso, Datos, Identidad, Red, Punto Final, Gobernanza, Recuperación, Incidentes y Gestión de Vulnerabilidades
- Gobernanza de Azure
- Crear, asignar e interpretar políticas de seguridad e iniciativas en Azure Policy
- Azure Blueprints
- Configurar ajustes de seguridad mediante Azure Blueprint
- Implementar infraestructuras seguras mediante una zona de aterrizaje (landing zone)
- Azure Key Vault

Contenido

- Seguridad de Azure Key Vault
- Autenticación en Azure Key Vault
- Crear y configurar un Azure Key Vault
- Recomendar cuándo usar un Módulo de Seguridad de Hardware (HSM) dedicado
- Configurar el acceso a Key Vault, incluidas las políticas de acceso al almacén y el control de acceso basado en roles de Azure
- Administrar certificados, secretos y claves
- Configurar la rotación de claves
- Configurar la copia de seguridad y recuperación de certificados, secretos y claves
- Implementar controles de seguridad para proteger copias de seguridad
- Implementar controles de seguridad para la gestión de activos

Módulo 109– Administración de la posición de seguridad mediante Microsoft Defender for Cloud

- Implementar Microsoft Defender para la Nube
- Identificación y corrección de riesgos de seguridad mediante el inventario y la puntuación de seguridad de Microsoft Defender for Cloud
- Evaluación del cumplimiento con marcos de seguridad y Microsoft Defender for Cloud
- Agregar estándares regulatorios y del sector a Microsoft Defender for Cloud
- Incorporación de iniciativas personalizadas a Microsoft Defender for Cloud
- Conexión de entornos de nube híbrida y multinube a Microsoft Defender for Cloud
- Identificación y supervisión de recursos externos mediante la administración de superficies expuestas a ataques externos de Microsoft Defender

Módulo 110 – Configuración y administración de la protección contra amenazas mediante Microsoft Denfender for Cloud

- Habilitación de los servicios de protección de cargas de trabajo en Microsoft Defender for Cloud
- Configurar Microsoft Defender para servidores
- Configuración de Microsoft Defender para Azure SQL Database
- Seguridad de contenedores en Microsoft Defender para contenedores
- Factores de amenaza de Kubernetes administrado
- Arquitectura de Defender para contenedores
- Configuración de componentes de Microsoft Defender para contenedores
- Evaluaciones de vulnerabilidades para Azure
- Defender para Storage
- Examen de malware en Defender para Storage
- Detección de amenazas a datos confidenciales
- Implementación de Microsoft Defender para Storage

Contenido

- Habilitación de la configuración de la directiva integrada de Azure
- Microsoft Defender for Cloud DevOps Security
- Soporte y requisitos previos de DevOps Security
- Posición de seguridad del entorno de DevOps
- Conexión del entorno de laboratorio de GitHub a Microsoft Defender for Cloud
- Configuración de la acción de GitHub de DevOps de seguridad de Microsoft
- Administración de alertas de seguridad y respuesta a ellas en Microsoft Defender for Cloud
- Configuración de la automatización de flujos de trabajo con Microsoft Defender for Cloud
- Evaluación de exámenes de vulnerabilidades de Microsoft Defender para servidores

Módulo 111 – Configuración y administración de soluciones de automatización y supervisión de seguridad

- Administración de alertas de seguridad y respuesta a ellas en Microsoft Defender for Cloud
- Configuración de la automatización de flujos de trabajo con Microsoft Defender for Cloud
- Planes de retención de registros en Microsoft Sentinel
- Alertas e incidentes de Microsoft Sentinel
- Configuración de conectores de datos en Microsoft Sentinel
- Habilitar reglas de análisis en Microsoft Sentinel
- Configuración de la automatización en Microsoft Sentinel
- Automatización de la respuesta a amenazas con Microsoft Sentinel

Módulo 112 – Introducción a los marcos de procedimientos recomendados y la confianza cero

- Introducción a los procedimientos recomendados.
- Introducción a Zero trust.
- Iniciativas de Zero trust.
- Pilares tecnológicos de Zero trust, parte 1.
- Pilares tecnológicos de Zero trust, parte 2.

Módulo 113 – Diseño de soluciones que se alineen con Cloud Adoption Framework (CAF) y el marco de buena arquitectura (WAF)

- Definición de una estragegia de seguridad.
- Introducción a Cloud Adoption Framwork.
- Metodología de seguridad de Cloud Adoption Framwork.
- Introducción a las zonas de aterrizaje de Azure.
- Diseño de seguridad con zonas de aterrizaje de Azure.
- Introducción al Marco de buena arquitectura.
- Pilar de seguridad del Marco de buena arquitectura.

Contenido

Módulo 114 – Diseño de soluciones que se alineen con la Arquitectura de referencia de ciberseguridad de Microsoft (MCRA) y Microsoft Cloud Security Benchmark (MCSB)

- Introducción a la Arquitectura de referencia de ciberseguridad de Microsoft y Cloud Security Benchmark.
- Diseñar soluciones con procedimientos recomendados para funcionalidades y controles,
- Diseño de soluciones con procedimientos recomendados para la protección contra ataques.

Módulo 115 – Diseño de una estrategia de resistencia para ciberamenazas comunes, como el ransonmware

- Patrones comunes de ciberamenazas y ataques.
- Compatibilidad con la resistencia empresarial.
- Protección contra ransomeware.
- Configuraciones de seguridad para las copias de seguridad y la restauración.
- Actualizaciones de seguridad.

Módulo 116 – Caso práctico: Diseño de soluciones que se alineen con los procedimientos recomendados de seguridad y las prioridades

- Descripción del caso práctico.
- Respuestas de caso práctico.
- Tutorial conceptual.
- Tutorial técnico.

Módulo 117 – Diseño de soluciones para el cumplimiento normativo

- Introducción al cumplimiento normativo.
- Traducción de los requisitos de cumplimiento en una solución de seguridad.
- Abordar los requisitos de cumplimiento con Microsoft Purview.
- Abordar los requisitos de privacidad con Microsoft Priva.
- Abordar los requisitos de seguridad y cumplimiento con Azure Policy.
- Evaluación del cumplimiento de la infraestructura con Defender for Cloud.

.

Contenido

Módulo 118 – Diseño de soluciones para la administración de identidades y acceso

- Diseño de estrategias de acceso en entornos de nube, híbridos y multinube (incluido Microsoft Entra ID).
- Diseño de una solución para identidades externas.
- Diseño de estrategias modernas de autenticación y autorización.
- Alineación del acceso condicional y la Confianza cero.
- Especificación de requisitos para proteger los Servicios de dominio de Active Directory (AD DS).
- Diseñar una solución para administrar secretos, claves y certificados.

Módulo 119 – Diseño de soluciones para proteger el acceso con privilegios

- Introducción al acceso con privilegios.
- Modelo de acceso empresarial.
- Diseño de soluciones de gobernanza de identidad.
- Diseño de una solución para proteger la administración de inquilinos.
- Diseño de una solución para la administración de derechos de infraestructura en la nube (CIEM).
- Diseño de una solución para estaciones de trabajo de acceso con privilegios y servicios bastión.

Módulo 120 – Diseño de soluciones para operaciones de seguridad

- Introducción a las operaciones de seguridad (SecOps).
- Diseño de funcionalidades de operaciones de seguridad en entornos híbridos y multinube.
- Diseño del registro y la auditoría centralizados.
- Diseño de soluciones de administración de eventos e información de seguridad (SIEM).
- Diseño de soluciones para detección y respuesta.
- Diseño de una solución para la orquestación de seguridad, automatización y respuesta (SOAR).
- Diseño de flujos de trabajo de seguridad.
- Diseño de la cobertura de detección de amenazas.

.

Contenido

Módulo 121 – Caso práctico: diseño de funcionalidades de operaciones de seguridad, identidad y cumplimiento

- Descripción del caso práctico.
- Respuestas del caso práctico.
- Tutoría conceptual.
- Tutorial técnico.

Módulo 122 – Diseñar soluciones para proteger Microsoft 365

- Introducción a la seguridad de Exchange, SharePoint, OneDrive y Teams.
- Evaluación de la posición de seguridad para las cargas de trabajo de colaboración y productividad.
- Diseño de una solución de Microsoft Defender XDR.
- Diseño de configuraciones y prácticas operativas para Microsoft 365.

Módulo 123 – Diseño de soluciones para proteger aplicaciones

- Introducción a la seguridad en las aplicaciónes.
- Diseño e implementación de estándares para proteger el desarrollo de aplicaciones.
- Evaluación de la posición de seguridad de las carteras de aplicaciones existentes.
- Evaluación de amenazas de aplicación con modelado de amenazas.
- Diseño de la estrategia de ciclo de vida de seguridad para aplicaciones.
- Acceso seguro para identidades de carga de trabajo.
- Diseño de una solución para la administración y seguridad de API.
- Diseño de una solución para el acceso seguro a las aplicaciones.

Módulo 124 – Diseño de soluciones para proteger los datos una organización

- Introducción a la seguridad de los datos.
- Diseño de una solución para la detección y clasificación de datos mediante Microsoft Purview.
- Diseño de una solución para la protección de los datos.
- Diseño de la seguridad de datos para cargas de trabajo de Azure.
- Diseño de la seguridad para Azure Storage.
- Diseño de una solución de seguridad con Microsoft Defender para SQL y Microsoft Defender para Storage.

Contenido

Módulo 125 – Caso práctico: diseño de soluciones de seguridad para aplicaciones y datos

- Descripción del caso práctico.
- Respuestas del caso práctico.
- Tutoría conceptual.
- Tutorial técnico.

Módulo 126– Especificación de los requisitos para proteger los servicios SaaS, PaaS e IaaS

- Introducción a la seguridad de SaaS, PaaS e IaaS.
- Especificación de las líneas de base de seguridad para los servicios SaaS, PaaS e IaaS.
- Especificación de requisitos de seguridad para cargas de trabajo web.
- Especificar los requisitos de seguridad para contenedores y la orquestación de contenedores.

Módulo 127 – Diseño de soluciones para la administración de la administración de la posición de seguridad en entornos híbridos y multinube

- Diseño de soluciones para la administración de la posición de seguridad en entornos híbridos y multinube.
- Evaluación de la posición de seguridad mediante Microsoft Cloud Security Benchmark.
- Diseño de la administración de la posición integrada y la protección de la carga de trabajo.
- Evaluación de la posición de seguridad mediante Microsoft Defender for Cloud.ç
- Evaluación de la posición con la puntuación de seguridad de Microsoft Defender for Cloud.
- Diseño de las protecciones de las cargas de trabajo en la nube con Microsoft Defender for Cloud.
- Integración de entornos híbridos y multinube con Azure Arc.
- Diseño de una solución para administrar la superficie expuesta a ataques externos.

Contenido

Módulo 128 – Diseño de soluciones para proteger los puntos de conexión de cliente y servidor

- Introducción a la seguridad de los puntos de conexión.
- Especificación de los requisitos de seguridad del servidor,
- Especificación de los requisitos para dispositivos móviles y clientes.
- Especificación de los requisitos de seguridad de Internet de las cosas (IoT) y los dispositivos insertados.
- Tecnología operativa segura (OT) y sistemas de control industrial (ICS) con Microsoft Defender para IoT.
- Especificación de líneas de base de seguridad para puntos de conexión de servidor y de cliente.
- Diseño de una solución para el acceso remoto seguro.

Módulo 129– Diseño de soluciones de para la seguridad de red

- Diseñar soluciones para la segmentación de la red.
- Diseño de soluciones para el filtrado del tráfico con grupos de seguridad de red.
- Diseño de soluciones para la administración de la posición de red.

Módulo 130 – Caso práctico: Diseño de soluciones de seguridad para la infrastructura

- Descripción del caso práctico.
- Respuestas de caso práctico.
- Tutorial conceptual.

GADESOFT

¿Tienes alguna duda o quieres saber más sobre nuestros cursos?

¡Contáctanos!

91 510 23 90

info@gadesoft.com

https://www.gadesoft.com/

C/ Clara del rey, 14, 28002 Madrid