Tel. +39 02 365738
info@overneteducation.it
www.overneteducation.it

MS-500T00
Microsoft 365 Security Administration

Durata: 4 gg

Descrizione

In questo corso imparerete come rendere sicuro l'accesso degli utenti alle risorse della vostra organizzazione. Il corso tratta la protezione della password utente, l'autenticazione a più fattori, come abilitare Azure Identity Protection, come impostare e utilizzare Azure AD Connect e introduce all'accesso condizionato in Microsoft 365.
Imparerai le tecnologie di protezione dalle minacce che aiutano a proteggere il tuo ambiente Microsoft 365. In particolare, imparerai a conoscere i vettori delle minacce e le soluzioni di sicurezza Microsoft per mitigare le minacce. Verranno fornite informazioni su Secure Score, protezione Exchange Online, Azure Advanced Threat Protection, Windows Defender Advanced Threat Protection e gestione delle minacce. In questo corso imparerete a conoscere le tecnologie di protezione delle informazioni che aiutano a proteggere il vostro ambiente Microsoft 365.
Questo corso tratta dei contenuti gestiti con i diritti di informazione, della crittografia dei messaggi, nonché delle etichette, delle politiche e delle regole che supportano la prevenzione della perdita di dati e la protezione delle informazioni. In questo corso imparerete a conoscere l'archiviazione e la conservazione in Microsoft 365, nonché la governance dei dati e come condurre ricerche e indagini sui contenuti. Questo corso tratta delle politiche di conservazione dei dati e dei tag, della gestione dei record locali per SharePoint, della conservazione della posta elettronica e di come condurre ricerche sui contenuti che supportano le indagini di eDiscovery.

A chi è rivolto?

Il Microsoft 365 Security Administrator collabora con il Microsoft 365 Enterprise Administrator, le parti aziendali interessate e altri amministratori di carichi di lavoro per pianificare e implementare strategie di sicurezza e verificare che le soluzioni siano conformi ai criteri e ai regolamenti dell’organizzazione.
Questo ruolo protegge in modo proattivo gli ambienti aziendali Microsoft 365. Le responsabilità comprendono la risposta alle minacce, l'implementazione, la gestione e il monitoraggio delle soluzioni di sicurezza e conformità per l'ambiente Microsoft 365. Rispondono agli incidenti, alle indagini e all'applicazione della governance dei dati. L'amministratore della sicurezza Microsoft 365 ha familiarità con i carichi di lavoro Microsoft 365 e gli ambienti ibridi. Questo ruolo ha forti competenze ed esperienze in materia di protezione dell'identità, protezione delle informazioni, protezione dalle minacce, gestione della sicurezza e governance dei dati.

Prerequisiti

Gli studenti che intendono seguire questo corso devono già possedere le seguenti competenze:

- •Comprensione concettuale di base di Microsoft Azure.
- •Esperienza con i dispositivi Windows 10.
- •Esperienza con Office 365.
- •Comprensione di base dell'autorizzazione e dell'autenticazione.
- •Conoscenza di base delle reti di computer.
- •Conoscenza di base della gestione dei dispositivi mobili.

Contenuti

Modulo 1: Protezione di utenti e gruppi

Questo modulo spiega come gestire gli account utente e i gruppi in Microsoft 365. Vi introduce alla gestione delle identità privilegiate in Azure AD così come alla protezione delle identità. Il modulo pone le basi per il resto del corso.

Lezioni

- •Concetti di gestione dell'identità e degli accessi
- •Sicurezza Zero Trust
- •Account dell’utente in Microsoft 365
- •Ruoli di amministratore e gruppi di sicurezza in Microsoft 365
- •Gestione della password in Microsoft 365
- •Protezione identità di Azure AD

Lab : Inizializzare il tuo tenant di prova

- •Impostare il proprio tenant Microsoft 365

Lab : Configurare la gestione delle identità privilegiate

- •Scoprire e gestire le risorse Azure
- •Assegnare ruoli Directory
- •Attivare e disattivare I ruoli PIM
- •Ruoli della Directory (Generale)
- •Flussi di risorse del PIM
- •Visualizzare la cronologia degli audit per I ruoli Azure AD in PIM

Al termine di questo modulo gli studenti saranno in grado di:

- •Creare e gestire gli account utente.
- •Descrivere e utilizzare i ruoli amministrativi di Microsoft 365.
- •Pianificare le politiche e l'autenticazione delle password.
- •Descrivere i concetti di sicurezza Zero Trust
- •Implementare l'autenticazione multi-fattore in Office 365.
- •Attivare la protezione dell'identità Azure

Modulo 2: Sincronizzazione dell'identità

Questo modulo spiega i concetti relativi alla sincronizzazione delle identità per Microsoft 365. In particolare, si concentra su Azure AD Connect e sulla gestione della sincronizzazione delle directory per garantire che le persone giuste si colleghino al vostro sistema Microsoft 365.

Lezioni

- •Introduzione alla sincronizzazione delle identità
- •Pianificare per Azure AD Connect
- •Implementare Azure AD Connect
- •Gestire identità sincronizzate
- •Introduzione alle identità federate

Laboratorio : Implementare la sincronizzazione delle identità

- •Impostare la vostra organizzazione per la sincronizzazione delle identità

Al termine di questo modulo gli studenti saranno in grado di:

- •Descrivere le opzioni di autenticazione per Microsoft 365.
- •Spiegare la sincronizzazione delle directory.
- •Pianificare la sincronizzazione delle directory.
- •Descrivere e utilizzare Azure AD Connect.

•Configurare i prerequisiti di Azure AD Connect.
•Gestire utenti e Gruppi con la sincronizzazione delle directory.
•Descrivere la federazione di Active Directory.

Modulo 3: Gestione degli accessi

Questo modulo spiega l'accesso condizionato per Microsoft 365 e come può essere utilizzato per controllare l'accesso alle risorse della propria organizzazione. Il modulo spiega anche il Role Based Access Control (RBAC) e le soluzioni per l'accesso esterno.

Lezioni

•Accesso condizionale
•Gestire l'accesso ai dispositivi
•Controllo dell’accesso basato sui ruoli (RBAC)
•Soluzioni per l’accesso esterno

Lab : Utilizzare l'accesso condizionato per abilitare l'MFA

•Pilota di autenticazione MFA (richiedere MFA per applicazioni specifiche)
•Accesso condizionato MFA (completare un roll out MFA)

Al termine di questo modulo gli studenti saranno in grado di:

•Descrivere il concetto di accesso condizionale.
•Descrivere e utilizzare le politiche di accesso condizionato.
•Pianificare la conformità dei dispositivi.
•Configurare utenti e gruppi condizionali.
•Configurare il controllo di accesso basato sul ruolo

Modulo 4: Sicurezza in Microsoft 365

Questo modulo spiega le varie minacce di cyber-attacco esistenti. Ti introduce poi alle soluzioni Microsoft utilizzate per mitigare tali minacce. Il modulo termina con una spiegazione del Microsoft Secure Score e di come può essere utilizzato per valutare e segnalare la postura di sicurezza delle vostre organizzazioni.

Lezioni

•Vettori di minacce e violazioni di dati
•Strategia e principi della sicurezza
•Soluzioni di sicurezza in Microsoft 365
•Microsoft Secure Score

Lab : Utilizzare Microsoft Secure Score

•Migliorare il proprio punteggio di sicurezza nel Microsoft 365 Security Center

Al termine di questo modulo gli studenti saranno in grado di:

•Descrivi diverse tecniche che gli aggressori utilizzano per compromettere gli account degli utenti tramite e-mail.
•Descrivere le tecniche che gli aggressori utilizzano per ottenere il controllo delle risorse.
•Elencare i tipi di minacce che possono essere evitate utilizzando Exhange Online Protection e Office 365 ATP.
•Descrivere i vantaggi di Secure Score e quali tipi di servizi possono essere analizzati.
•Descrivere come utilizzare Secure Score per identificare le lacune nella propria attuale situazione di sicurezza Microsoft 365.

Modulo 5: Protezione avanzata dalle minacce

Questo modulo spiega le varie tecnologie e servizi di protezione dalle minacce disponibili per Microsoft 365. Il modulo copre la protezione dei messaggi attraverso Exchange Online Protection, Azure Advanced Threat Protection e Windows Defender Advanced Threat Protection.

Lezioni

- •Exchange Online Protection
- •Office 365 Advanced Threat Protection
- •Gestione degli allegati sicuri
- •Gestione dei link sicuri
- •Azure Advanced Threat Protection
- •Microsoft Defender Advanced Threat Protection

Lab : gestisci Microsoft 365 Security Services

- •Implementare i criteri ATP

Al termine di questo modulo gli studenti saranno in grado di:

- •Descrivere il flusso anti-malware mentre l'email viene analizzata da Exchange Online Protection.
- •Descrivere come Safe Attachments viene utilizzato per bloccare il malware zero-day negli allegati e-mail e nei documenti.
- •Descrivere come I collegamenti sicuri proteggono gli utenti da URL dannosi incorporati nella posta elettronica e nei documenti che puntano a
- •Configurare la protezione avanzata delle minacce di Azure.
- •Configurare Windows Defender ATP.

Modulo 6: Gestione delle minacce

Questo modulo spiega il Microsoft Threat Management che fornisce gli strumenti per valutare e affrontare le minacce informatiche e formulare le risposte. Imparererai a utilizzare il cruscotto di sicurezza e Azure Sentinel per Microsoft 365. Il modulo spiega e configura anche Microsoft Advanced Threat Analytics.

Lezioni

- •Utilizzare il cruscotto di sicurezza
- •Indagine e risposta alle minacce di Microsoft 365
- •Azure Sentinel per Microsoft 365
- •Configurare un’analisi avanzata delle minacce

Lab : Utilizzo del simulatore di attacco

- •Condurre un attacco di Spear phishing simulato
- •Condurre attacchi con password simulate

Al termine di questo modulo gli studenti saranno in grado di:

- •Descrivere come Threat Explorer può essere utilizzato per indagare sulle minacce e contribuire a proteggere il vostro tenant.
- •Descrivere come il cruscotto di sicurezza fornisce ai dirigenti di livello C una panoramica dei rischi e delle tendenze più importanti.
- •Descrivere cos'è l'Advanced Thread Analytics (ATA) e quali sono i requisiti necessari per la sua implementazione.
- •Configurare l'analisi avanzata delle minacce.
- •Utilizzare il simulatore di attacco in Microsoft 365.
- •Descrivere come Azure Sentinel può essere utilizzato per Microsoft 365.

Modulo 7: Mobilità

Questo modulo si concentra sulla sicurezza dei dispositivi e delle applicazioni mobili. Imparererai a conoscere la gestione dei dispositivi mobili e come funziona con Microsoft Intune. Imparererai anche come Intune e Azure AD possono essere utilizzati per proteggere le applicazioni mobili.

Lezioni

- •Pianificare la gestione di applicazioni mobili

- •Pianificare la gestione di dispositivi mobili
- •Implementare la gestione dei dispositivi mobili
- •Registrare i dispositivi alla gestione dei dispositivi mobili

Lab : Configurare Azure AD per Intune

- •Abilitare gestione dispositivi
- •Configurare Azure AD per Intune
- •Creare di politiche Intune

Al termine di questo modulo gli studenti saranno in grado di:

- •Descrivere le considerazioni relative alle applicazioni mobili.
- •Utilizzare Intune per gestire le applicazioni mobili.
- •Gestire i dispositivi con MDM.
- •Configurare i domini per MDM.
- •Gestire le politiche di sicurezza dei dispositivi.
- •Registrare i dispositivi su MDM.
- •Configurare un ruolo di gestione della registrazione dei dispositivi.

Modulo 8: Protezione delle informazioni

Il modulo spiega come implementare Azure Information Protection e Windows Information Protection.

Lezioni

- •Concetti di protezione delle informazioni
- •Protezione delle informazioni di Azure
- •Protezione avanzata delle informazioni
- •Protezione delle informazioni di Windows

Lab : Implementare la protezione delle informazioni di Azure e la protezione delle informazioni di Windows

- •Implementazione di Azure Information Protection
- •Implementazione di Windows Information Protection

Al termine di questo modulo gli studenti saranno in grado di:

- •Configurare le etichette e le politiche per la Protezione delle Informazioni di Azure.
- •Configurare le impostazioni avanzate del servizio AIP per i modelli dei servizi di gestione dei diritti (RMS).
- •Pianificare l'implementazione delle politiche di protezione delle informazioni di Windows.

Modulo 9: Gestione dei diritti e crittografia

Questo modulo spiega la gestione dei diritti di informazione in Exchange e SharePoint. Il modulo descrive anche le tecnologie di crittografia utilizzate per proteggere i messaggi.

Lezioni

- •Gestione dei diritti di informazione
- •Estensione sicura della posta su Internet Multipurpose
- •Crittografia dei messaggi di Office 365

Lab: Configurare la crittografia dei messaggi di Office 365

- •Configurare la crittografia dei messaggi di Office 365
- •Convalidare la gestione dei diritti di informazione

Al termine di questo modulo gli studenti saranno in grado di:

- •Descrivere le varie opzioni di crittografia di Microsoft 365.
- •Descrivere l'uso di S/MIME.
- •Descrivere e abilitare la crittografia dei messaggi di Office 365.

Modulo 10: Prevenzione della perdita di dati

Questo modulo si concentra sulla prevenzione della perdita di dati in Microsoft 365. Imparererai come creare

politiche, modificare le regole e personalizzare le notifiche degli utenti per proteggere i propri dati.
Lezioni
- •Spiegazione della prevenzione della perdita dei dati
- •Criteri della prevenzione della perdita dei dati
- •Criteri personalizzati DLP
- •Creare una politica DLP per proteggere i documenti
- •Suggerimenti dei criteri

Lab : Implementare le politiche di prevenzione della perdita di dati (Data Loss Prevention)
- •Gestire le politiche DLP
- •Test delle MRM and DLP Policies

Al termine di questo modulo gli studenti saranno in grado di:
- •Descrivere la prevenzione della perdita dei dati (DLP).
- •Usare modelli di politiche per implementare le politiche DLP per le informazioni di uso comune.
- •Configurare le regole corrette per la protezione dei contenuti.
- •Descrivere come modificare le regole esistenti delle politiche DLP.
- •Configurare l'opzione di sovrascrittura dell'utente su una regola DLP.
- •Spiegare come SharePoint Online crea proprietà scansionate da documenti.

Modulo 11: Sicurezza delle applicazioni cloud
Questo modulo si concentra sulla sicurezza delle applicazioni cloud in Microsoft 365. Il modulo spiegherà la scoperta del cloud, i connettori delle app, i criteri e gli avvisi. Imparererai come funzionano queste funzioni per proteggere le proprie applicazioni cloud.
Lezioni
- •Spiegazione della sicurezza delle applicazioni cloud
- •Utilizzo delle informazioni della sicurezza delle applicazioni cloud

Al termine di questo modulo gli studenti saranno in grado di:
- •Descirvere Cloud App Security.
- •Spiegare come implementare Cloud App Security.
- •Controllare le vostre applicazioni cloud con i criteri.
- •Utilizzare il catalogo delle applicazioni cloud.
- •Utilizzare Cloud App Catalog.
- •Gestire le autorizzazioni delle applicazioni cloud.

Modulo 12: Conformità in Microsoft 365
Questo modulo si concentra sulla governance dei dati in Microsoft 365. Il modulo vi introdurrà al Compliance Manager e discuterà di regolamento globale sulla protezione dei dati (GDPR).
Lezioni
- •Pianificare per i requisiti di conformità
- •Costruire muri etici in Exchange Online
- •Gestire la conservazione nella posta elettronica
- •Risoluzione dei problemi di governance dei dati

Al termine di questo modulo gli studenti saranno in grado di:
- •Pianificare ruoli di sicurezza e di conformità.
- •Descrivere ciò che è necessario considerare per GDPR.
- •Descrivere cos'è un muro etico in Exchange e come funziona.
- •Lavorare con i tag di ritenzione nelle caselle di posta.
- •Descrivere le politiche di conservazione con i messaggi e-mail e le cartelle di posta elettronica.

•Spiegare come viene calcolato il periodo di ritenzione degli elementi.
•Riparare le politiche di ritenzione che non funzionano come previsto.

Modulo 13: Archiviazione e conservazione

Questo modulo spiega i concetti relativi alla conservazione e all'archiviazione dei dati per Microsoft 365, compresi Exchange e SharePoint.

Lezioni

•Archiviazione in Microsoft 365
•Conservazione in Microsoft 365
•Politiche di ritenzione nel Microsoft 365 Compliance Center
•Archiviazione e conservazione in Exchange
•Gestione dei record in loco in SharePoint

Lab : Conformità e ritenzione

•Inizializzare la conformità
•Configurare le politiche e i tag di ritenzione

Al termine di questo modulo gli studenti saranno in grado di:

•Descrivere la differenza tra gestione dei file e archiviare localmente.
•Spiegare come vengono archiviati i dati su Exchange.
•Spiegare come funziona una politica di ritenzione.
•Creare una politica di conservazione.
•Attivare e disattivare l'archiviazione in loco.
•Creare tag utili di conservazione.

Modulo 14: Ricerca e indagine sui contenuti

Questo modulo si concentra sulla ricerca e sulle indagini relative ai contenuti. Il modulo tratta di come utilizzare eDiscovery per condurre indagini avanzate sui dati Microsoft 365. Tratta anche dei registri di audit e delle richieste di dati GDPR degli interessati.

Lezioni

•Ricerca di contenuti
•Indagini sul registro di audit
•eDiscovery avanzato

Lab : gestire ricerche e indagini

•Esaminare i vostri dati Microsoft 365
•Condurre una richiesta di dati di un soggetto

Al termine di questo modulo gli studenti saranno in grado di:

•Descrivere come utilizzare la ricerca dei contenuti.
•Progettare una ricerca di contenuti.
•Configurare il filtraggio dei permessi di ricerca.
•Configurare le politiche di audit.
•Inserire i criteri per la ricerca nel registro di audit.
•Descrivere l'eDiscovery avanzato in Microsoft 365.
•Visualizzare il registro eventi di eDiscovery avanzato.

Certificazioni

Il corso è propedeutico per i seguenti esami:

•MS-500 - Microsoft 365 Security Administrator