Pipeline

Pipeline is a Leading Learning Partners Association Member

MOC SC-5004 - DEFEND AGAINST CYBERTHREATS WITH MICROSOFT DEFENDER XDR

APPLIED SKILL

Durata	Prezzo	Orari	Calendario
0,5 giorni	350,00€ + IVA	9:00-13:00	

Questo corso SC-5004 - Defend against cyberthreats with Microsoft Defender XDR insegna ad implementare l'ambiente Microsoft Defender for Endpoint per gestire i dispositivi, eseguire indagini sugli endpoint, gestire gli incidenti in Defender XDR e utilizzare Advanced Hunting con Kusto Query Language (KQL) per rilevare minacce uniche.

Contenuti del corso

Mitigare gli incendi usando Microsoft Defender

- Usare il portale di Microsoft Defender
- Gestire gli eventi imprevisti
- Eseguire indagini sugli eventi imprevisti
- Gestire e analizzare gli avvisi
- Gestire le indagini automatizzate
- Usare il Centro operativo
- Esplorare la ricerca avanzata
- Analizzare i log di accesso di Microsoft Entra
- Informazioni su Microsoft Secure Score
- Esplorare l'analisi delle minacce
- Analizza report
- Configurare il portale di Microsoft Defender

Distribuire l'ambiente Microsoft Defender per endpoint

- Creare l'ambiente
- Informazioni sulla compatibilità e le funzionalità dei sistemi operativi
- Eseguire l'onboarding dei dispositivi
- Gestire l'accesso
- Creare e gestire i ruoli per il controllo degli accessi in base al ruolo
- Configurare gruppi di dispositivi

- Configurare le funzionalità avanzate dell'ambiente

Eseguire la configurazione per gli avvisi e i rilevamenti in Microsoft Defender per endpoint

- Configura le funzionalità avanzate
- Configurare le notifiche di avviso
- Gestire l'eliminazione degli avvisi
- Gestire gli indicatori

Configurare e gestire l'automazione con Microsoft Defender per endpoint

- Configura le funzionalità avanzate
- Gestire le impostazioni di caricamento dell'automazione e della cartella
- Configurare le funzionalità di indagine e correzione automatizzate
- Bloccare i dispositivi a rischio

Eseguire indagini sui dispositivi in Microsoft Defender per endpoint

- Usare l'elenco di inventario dei dispositivi
- Analizzare il dispositivo
- Usare il blocco secondo dati comportamentali
- Rilevare i dispositivi con l'individuazione dei dispositivi

Difendersi dalle minacce informatiche con gli esercizi del lab su Microsoft Defender XDR

- Configurare l'ambiente di Microsoft Defender XDR
- Distribuire Microsoft Defender per endpoint
- Mitigare gli attacchi con Microsoft Defender per endpoint

Partecipanti
Questo corso di formazione SC-5004 – Defend against cyberthreats with Microsoft Defender XDR si rivolge a analisti e desperti della sicurezza.

Obiettivi
Gli obiettivi di apprendimento di questo corso SC-5004 – Defend against cyberthreats with Microsoft Defender XDR sono:

- comprendere come il portale di Microsoft Defender offre una visualizzazione unificata degli incidenti della famiglia di prodotti Microsoft Defender
- comprendere come distribuire l'ambiente Microsoft Defender per endpoint, inclusi l'onboarding dei dispositivi e la configurazione della sicurezza
- saper configurare le impostazioni per gestire avvisi e notifiche
- saper configurare l'automazione in Microsoft Defender per endpoint tramite la gestione delle impostazioni dell'ambiente
- comprendere come ottenere informazioni dettagliate sui dispositivi

- comprendere come configurare Microsoft Defender XDR

Prerequisiti
Per partecipare con profitto a questo corso SC-5004 – Defend against cyberthreats with Microsoft Defender XDR è necessario avere:

- Esperienza nell'utilizzo del portale Microsoft Defender
- Conoscenza di base di Microsoft Defender for Endpoint
- Conoscenza di base di Microsoft Sentinel
- Esperienza nell'uso di Kusto Query Language (KQL) in Microsoft Sentinel

Lingua

Lingua utilizzata nel corso/dal docente: Italiano

Materiali e Bonus

Il corso include:

- **documentazione** didattica accessibile via web, di durata illimitata;
- un **attestato** di frequenza inviato via e-mail una settimana dopo il termine del corso.

Hai bisogno di chiarimenti o ulteriori informazioni?
Vuoi organizzare un corso personalizzato?
Chiamaci: 02/6074791 Scrivici: formazione@pipeline.it