Pipeline

Pipeline is a Leading Learning Partners Association Member

# MOC SC-200 - MICROSOFT SECURITY OPERATIONS ANALYST

CORSO CON DOCENTE

| Durata | Prezzo | Orari | Calendario |
|---|---|---|---|
| 4 giorni | 1.272,00€ – 1.590,00€ + IVA | | 05/10/2026 Aula Virtuale<br>01/12/2026 Aula Virtuale<br>08/06/2026 Aula Virtuale<br>03/08/2026 Aula Virtuale |

I partecipanti del **corso SC-200 Microsoft Security Operations Analyst** scopriranno come analizzare, rispondere e rilevare minacce usando Microsoft Sentinel, Microsoft Defender XDR e Microsoft Defender per il cloud. In questo corso verrà descritto come mitigare le minacce informatiche usando queste tecnologie. In particolare, verrà configurato e usato Microsoft Sentinel e verrà usato il linguaggio di query Kusto (KQL) per eseguire il rilevamento, l'analisi e la creazione di report.

Il corso è stato progettato per le persone che lavorano in un ruolo lavorativo inerente la sicurezza informatica e aiuta a prepararsi per l'esame di certificazione SC-200: Microsoft Security Operations Analyst

Contenuti del corso

## Attenuare le minacce con Microsoft Defender XDR

- Introduzione alla protezione dalle minacce di Microsoft Defender XDR
- Mitigare gli incendi usando Microsoft Defender
- Correggere i rischi con Microsoft Defender per Office 365
- Gestire Microsoft Entra Identity Protection
- Proteggere l'ambiente con Microsoft Defender per identità
- Correggere i rischi con Microsoft Defender per Office 365
- Proteggere le app e i servizi cloud con Microsoft Defender for Cloud Apps

## Mitigare le minacce usando Microsoft Security Copilot

- Nozioni fondamentali sull'intelligenza artificiale generativa

- Descrivere Microsoft Security Copilot
- Descrivere le funzionalità di base di Microsoft Security Copilot
- Descrivi le esperienze integrate di Microsoft Security Copilot
- Esplorare i casi d'uso di Microsoft Security Copilot

### Mitigare le minacce con Microsoft 365 Defender

- Rispondere agli avvisi di prevenzione della perdita dei dati con Microsoft 365
- Gestire i rischi Insider in Microsoft Purview
- Ricerca e analisi con Microsoft Purview Audit
- Analizzare le minacce con la ricerca di contenuto in Microsoft Purview

### Mitigare le minacce con Microsoft Defender per endpoint

- Protezione dalle minacce con Microsoft Defender per Endpoint
- Distribuire l'ambiente Microsoft Defender per endpoint
- Implementare i miglioramenti della sicurezza di Windows con Microsoft Defender per endpoint
- Eseguire indagini sui dispositivi in Microsoft Defender per endpoint
- Eseguire azioni su un dispositivo con Microsoft Defender per endpoint
- Eseguire indagini sulle evidenze e sulle entità usando Microsoft Defender per endpoint
- Configurare e gestire l'automazione con Microsoft Defender per endpoint
- Eseguire la configurazione per gli avvisi e i rilevamenti in Microsoft Defender per endpoint
- Usare la gestione delle vulnerabilità in Microsoft Defender per endpoint

### Mitigare le minacce con Microsoft Defender per il cloud

- Pianificare le protezioni dei carichi di lavoro cloud con Microsoft Defender for Cloud
- Connettere asset di Azure a Microsoft Defender for Cloud
- Connettere risorse non Azure a Microsoft Defender for Cloud
- Gestire Cloud Security Posture Management
- Spiegare le protezioni dei carichi di lavoro cloud in Microsoft Defender per il cloud
- Correggere gli avvisi di sicurezza con Microsoft Defender for Cloud

### Creare query per Microsoft Sentinel con il linguaggio di query Kusto (KQL)

- Costruire istruzioni KQL per Microsoft Sentinel
- Analizzare i risultati delle query con KQL
- Compilare istruzioni multitabella usando KQL
- Usare i dati in Microsoft Sentinel tramite il linguaggio di query Kusto

### Configurare l'ambiente Microsoft Sentinel

- Introduzione a Microsoft Sentinel

- Creare e gestire le aree di lavoro di Microsoft Sentinel
- Eseguire query su log in Microsoft Sentinel
- Usare le watchlist in Microsoft Sentinel
- Utilizzare l'intelligence sulle minacce in Microsoft Sentinel
- Integrare Microsoft Defender XDR con Microsoft Sentinel

## Connettere i log a Microsoft Sentinel

- Connettere i dati a Microsoft Sentinel usando i connettori dati
- Connettere i servizi Microsoft a Microsoft Sentinel
- Connessione Da Microsoft Defender XDR a Microsoft Sentinel
- Connettere host Microsoft a Microsoft Sentinel
- Connettere i log Common Event Format a Microsoft Sentinel
- Connettere origini dati Syslog a Microsoft Sentinel
- Connettere gli indicatori di minaccia a Microsoft Sentinel

## Creare rilevamenti ed eseguire indagini con Microsoft Sentinel

- Rilevamento delle minacce con le analisi di Microsoft Sentinel
- Automazione in Microsoft Sentinel
- Risposta alle minacce con i playbook di Microsoft Sentinel
- Gestione degli eventi imprevisti di sicurezza in Microsoft Sentinel
- Identificare le minacce con l'analisi del comportamento
- Normalizzazione dei dati in Microsoft Sentinel
- Eseguire query, visualizzare e monitorare i dati in Microsoft Sentinel
- Gestire il contenuto in Microsoft Sentinel

## Eseguire la ricerca delle minacce in Microsoft Sentinel

- Spiegare la ricerca delle minacce in Microsoft Sentinel
- Ricerca delle minacce con Microsoft Sentinel
- Usare i processi di ricerca in Microsoft Sentinel
- Eseguire la ricerca delle minacce usando i notebook in Microsoft Sentinel

Obiettivi

Al termine del corso gli allievi saranno in grado di:

- mitigare le minacce usando Microsoft 365 Defender;
- attenuare le minacce utilizzando Azure Defener;
- attenuare le minacce usando Azure Sentinel.

Prerequisiti

Pipeline

Pipeline is a Leading Learning Partners Association Member

Per partecipare con profitto al **corso SC-200 Microsoft Security Operations Analyst** gli allievi dovrebbero essere in possesso dei seguenti prerequisiti:

- comprensione di base di Microsoft 365;
- comprensione fondamentale dei prodotti Microsoft per la sicurezza, la conformità e l'identità;
- familiarità con i servizi Azure, in particolare Azure SQL Database e Azure Storage;
- comprensione intermedia di Windows 10;
- familiarità con le macchine virtuali Azure e la rete virtuale;
- comprensione di base dei concetti di scripting.

Partecipanti

Il Microsoft Security Operations Analyst collabora con gli stakeholder organizzativi al fine di rendere sicuri i sistemi informatici dell'organizzazione. Il suo obiettivo è quello di ridurre il rischio rimediando rapidamente agli attacchi attivi nell'ambiente, consigliando miglioramenti alle pratiche di protezione dalle minacce e segnalando le violazioni delle politiche organizzative agli stakeholder appropriati. Le responsabilità includono la gestione delle minacce, il monitoraggio e la risposta, utilizzando una varietà di soluzioni.

Materiali e Bonus
Il corso MOC SC-200 – Microsoft Security Operations Analyst **include**:

- **un manuale ufficiale Microsoft Learning** (in lingua inglese) accessibile online, di durata **illimitata**;
- **un ambiente di laboratorio** con macchine virtuali accessibili online **per 180 giorni** dalla data del corso;
- un **attestato di frequenza** inviato via e-mail una settimana dopo il termine del corso.

Ed inoltre, se disponibile, un Kit di **Simulazione d'Esame** (Practice Test), accessibile **per 180 giorni** sul sito measureup.com, **del valore di 89 Euro**. (*da attivare entro tre mesi dal corso*)

measureup

**** L'edizione in promozione straordinaria per il CyberSecurity Month non include voucher e simulazione***

---

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