Idee e Valori al servizio delle Aziende

MICROSOFT SECURITY OPERATIONS ANALYST (SC-200)

Impara come esaminare, rispondere e scovare le minacce usando Microsoft Azure Sentinel, Azure Defender, e Microsoft 365 Defender. In questo corso imparerai come mitigare le minacce virtuali usando queste tecnologie. Nello specifico, configurerai e userai Azure Sentinel e utilizzerai anche Kusto Query Language (KQL) per eseguire identificazione, analisi e rendicontazione. Questo corso è stato pensato per coloro che occupano posizioni nell'ambito della Sicurezza delle Operazioni e prepara i discenti a prepararsi per l'esame SC-200: Microsoft Security Operations Analyst.

OBIETTIVI

A seguito del completamento del corso I partecipanti potranno:

- Spiegare come Microsoft Defender per Endpoint può porre rimedio ai rischi presenti nel tuo ambiente
- Creare un ambiente Microsoft Defender per Endpoint
- Configurare regole Riduzione della Superficie di Attacco su dispositivi Windows 10
- Eseguire azioni su un dispositivo che usa Microsoft Defender per Endpoint
- Esaminare domini e indirizzi IP su Microsoft Defender per Endpoint
- Esaminare account utente su Microsoft Defender per Endpoint
- Configurare impostazioni avvisi su Microsoft Defender per Endpoint
- Spiegare come il panorama delle minacce si sta evolvendo
- Condurre una caccia avanzata su Microsoft 365 Defender
- Gestire gli incidenti su Microsoft 365 Defender
- Spiegare come Microsoft Defender for Identity può porre rimedio ai rischi nel tuo ambiente
- Esaminare avvisi DLP su Microsoft Cloud App Security
- Spiegare i tipi di azioni che puoi intraprendere su un caso di gestione rischio interno.
- Configurare il provisioning automatico su Azure Defender
- Neutralizzare gli avvisi su Azure Defender
- Costruire istruzioni KQL
- Filtrare le ricerche in base all'ora dell'evento, la gravità, il dominio e altri dati rilevanti usando KQL
- Estrarre dati da stringhe non strutturate usando KQL

- Gestire uno spazio di lavoro Azure Sentinel
- Usare KQL per accedere alla watchlist su Azure Sentinel
- Gestire gli indicatori di minaccia su Azure Sentinel
- Spiegare le differenze di Common Event Format e il connettore Syslog su Azure Sentinel
- Connettere Azure Windows Virtual Machines a Azure Sentinel
- Configurare un agente di Analisi Registri per raccogliere eventi Sysmon
- Creare nuove regole analitiche e query usando la procedura guidata delle regole di analisi
- Creare una strategia per automatizzare la risposta a un incidente
- Usare query per scovare le minacce
- Osservare le minacce nel corso del tempo con livestream

DURATA DEL CORSO

4 giorni

DESTINATARI

Il Security Operations Analyst di Microsoft collabora con componenti aziendali per rendere sicuri i sistemi tecnologici di informazioni per le aziende. Il suo obiettivo è ridurre il rischio dell'azienda ponendo rapidamente rimedio agli attacchi attivi nell'ambiente, fornendo consigli su miglioramenti delle pratiche di protezione dalle minacce, e riportando politiche di violazione aziendale ai membri appropriati dell'azienda. Le sue responsabilità comprendono gestione delle minacce, monitoraggio, e risposta usando un insieme di soluzioni di sicurezza all'interno dell'ambiente. Il ruolo si concentra principalmente sull'esame, la risposta e la caccia alle minacce usando Microsoft Azure Sentinel, Azure Defender, Microsoft 365 Defender, e prodotti di sicurezza di terze parti. Visto che il Security Operations Analyst impiega l'output operativo di questi strumenti, è una componente critica nella configurazione e nella distribuzione di queste tecnologie.

PREREQUISITI

Prima di partecipare a questo corso, gli studenti devono avere:

- Comprensione di base di Microsoft 365
- Comprensione delle basi dei prodotti di sicurezza, conformità e identità di Microsoft
- Comprensione di livello intermedio di Windows 10
- Familiarità con i servizi Azure, in particolare Azure SQL Database e Azure Storage
- Familiarità con le macchine virtuali e le reti virtuali Azure

Comprensione di base dei concetti di scripting.

CONTENUTI

Il corso tratta i seguenti macro contentuti:

Modulo 1: Mitigare le minacce usando Microsoft Defender per Endpoint

Implementare la piattaforma Microsoft Defender per Endpoint per individuare, esaminare e rispondere alle minacce avanzate. Scopri come Microsoft Defender per Endpoint può aiutare la tua azienda a rimanere al sicuro. Impara come distribuire l'ambiente Microsoft Defender per Endpoint, comprendendo i dispositivi onboarding e la configurazione della sicurezza. Impara come esaminare gli incidenti e gli avvisi usando Microsoft Defender per Endpoints. Esegui delle cacce avanzate e richiedi un consulto con esperti delle minacce. Imparerai anche come configurare l'automazione su Microsoft Defender per Endpoint gestendo le impostazioni ambientali. Infine, scoprirai le vulnerabilità del tuo ambiente usando Threat and Vulnerability Management su Microsoft Defender per Endpoint.

Lezioni

- Proteggere dalle minacce con Microsoft Defender per Endpoint
- Distribuire l'ambiente Microsoft Defender per Endpoint
- Implementare miglioramenti di sicurezza su Windows 10 con Microsoft Defender per Endpoint
- Gestire avvisi e incidenti su Microsoft Defender per Endpoint
- Eseguire esami di dispositivi su Microsoft Defender per Endpoint
- Eseguire azioni su un dispositivo usando Microsoft Defender per Endpoint
- Eseguire esami di evidenze ed entità usando Microsoft Defender per Endpoint
- Configurare e gestire l'automazione usando Microsoft Defender per Endpoint
- Configurare avvisi e rilevamento su Microsoft Defender per Endpoint
- Utilizzare Threat and Vulnerability Management su Microsoft Defender per Endpoint

Lab : Mitigare le minacce usando Microsoft Defender per Endpoint

- Distribuire Microsoft Defender per Endpoint
- Mitigare gli Attacchi usando Defender per Endpoint

Dopo aver completato questo moduli, gli studenti saranno in grado di:

- Definire le potenzialità di Microsoft Defender per Endpoint
- Configurare impostazioni di ambiente su Microsoft Defender per Endpoint
- Configurare regole di Riduzione della Superficie di Attacco su dispositivi Windows 10
- Esaminare avvisi su Microsoft Defender per Endpoint
- Illustrare informazioni forensi su un dispositivo raccolte da Microsoft Defender per Endpoint
- Condurre raccolte dati forensi usando Microsoft Defender per Endpoint
- Esaminare account utente su Microsoft Defender per Endpoint
- Gestire impostazioni di automazione su Microsoft Defender per Endpoint
- Gestire indicatori su Microsoft Defender per Endpoint
- Descrivere la Threat and Vulnerability Management su Microsoft Defender per Endpoint

Modulo 2: Mitigare le minacce usando Microsoft 365 Defender

Analizzare i dati delle minacce nei vari domini e porre rapidamente rimedio alle minacce con la strumentazione integrata e l'automazione su Microsoft 365 Defender. Scopri le minacce informatiche e come i nuovi strumenti di protezione dalle minacce di Microsoft proteggono gli utenti della tua azienda, dispositivi e dati. Usa il rilevamento avanzato e la risoluzione delle minacce basate sull'identificazione per proteggere le tue identità e applicazioni Azure Active Directory dalla compromissione.

Lezioni

- introduzione alla protezione dalle minacce con Microsoft 365
- Mitigare gli incidente usando Microsoft 365 Defender
- Proteggere le tue identificazioni con Azure AD Identity Protection
- Porre rimedio ai rischi con Microsoft Defender per Office 365
- Salvaguardare il tuo ambiente con Microsoft Defender for Identity
- Rendere sicure le tue app e servizi cloud con Microsoft Cloud App Security
- Rispondere agli avvisi di prevenzione da perdita dati usando Microsoft 365
- Gestire il rischio interno su Microsoft 365

Lab : Mitigare le minacce usando Microsoft 365 Defender

- Mitigare gli Attacchi con Microsoft 365 Defender

Dopo aver completato questo modulo, gli studenti saranno in grado di:

- Spiegare come si sta evolvendo il panorama delle minacce.
- Gestire gli incidenti su Microsoft 365 Defender
- Condurre delle ricerche avanzate su Microsoft 365 Defender
- Illustrare le funzioni di esame e riparazione di Azure Active Directory Identity Protection.
- Definire le potenzialità di Microsoft Defender per Endpoint.
- Spiegare come Microsoft Defender per Endpoint può porre rimedio ai rischi nel tuo ambiente.
- Definire la struttura Cloud App Security
- Spiegare come Cloud Discovery ti aiuta a vedere cosa succede nella tua azienda

Modulo 3: Mitigare le minacce usando Azure Defender

Usa Azure Defender integrato con Azure Security Center, per la protezione e sicurezza di Azure, cloud ibrido, carichi di lavoro in sede. Scopri gli obiettivi del rapporto tra Azure Defender, Azure Defender e Azure Security Center, e come abilitare Azure Defender. Scoprirai anche le modalità di protezione e individuazione fornite da Azure Defender per ogni carico di lavoro su cloud. Impara come aggiungere le potenzialità di Azure Defender al tuo ambiente ibrido.

Lezioni

- Pianificare la protezione di carichi di lavoro su cloud usando Azure Defender
- Spiegare la protezione di carichi di lavoro su cloud su Azure Defender
- Connettere le risorse di Azure a Azure Defender
- Connettere le risorse non-Azure a Azure Defender
- Risolvere gli avvisi di sicurezza usando Azure Defender

Lab : Mitigare le minacce usando Azure Defender

- Distribuire Azure Defender
- Mitigare gli Attacchi con Azure Defender

Dopo aver completato questo modulo, gli studenti saranno in grado di:

- Illustrare le funzionalità di Azure Defender
- Spiegare le funzionalità di Azure Security Center
- Spiegare quali carichi di lavoro sono protetti da Azure Defender
- Spiegare il funzionamento della protezione di Azure Defender
- Configurare il provisioning automatico su Azure Defender
- Illustrare il provisioning manuale su Azure Defender
- Connettere macchine non-Azure a Azure Defender
- Descrivere avvisi su Azure Defender
- Risolvere avvisi su Azure Defender
- Automatizzare le risposte su Azure Defender

Modulo 4: Creare query per Azure Sentinel usando Kusto Query Language (KQL)

Scrivi istruzioni Kusto Query Language (KQL) in query di dati di registro per eseguire rilevamenti, analisi e rendicontazione su Azure Sentinel. Questo modulo si concentrerà sugli operatori più utilizzati. L'esempio delle istruzioni KQL statements esemplificherà la sicurezza relativa alle query delle tabelle. KQL è il linguaggio di query usato per eseguire l'analisi di dati al fine di creare statistiche, cartelle di lavoro e eseguire una caccia su Azure Sentinel. Impara come la struttura dell'istruzione di base KQL fornisce le fondazioni per costruire delle istruzioni più complesse. Impara in che modo sintetizzare e visualizzare dati con un'istruzione KQL fornisce le basi per costruire il rilevamento su Azure Sentinel. Impara come usare il Linguaggio Kusto Query (KQL) per manipolare stringhe di dati assorbite da fonti di registri.

Lezioni

- Costruire istruzioni KQL per Azure Sentinel
- Analizzare risultati di query usando KQL
- Costruire istruzioni multi-tabella usando KQL
- Lavorare con i dati su Azure Sentinel usando Kusto Query Language

Lab : Creare query per Azure Sentinel usando Kusto Query Language (KQL)

- Costruire Istruzioni KQL di Base
- Analizzare i risultati di query usando KQL
- Costruire istruzioni multi-tabella usando KQL
- Lavorare con stringhe di dati usando istruzioni KQL

Dopo aver completato questo modulo, gli studenti saranno in grado di:

- Costruire istruzioni KQL
- Ricercare file di log per la sicurezza degli eventi usando KQL
- Filtrare le ricerche in base all'ora dell'evento, la gravità, il dominio e altri dati rilevanti usando KQL
- Sintetizzare i dati usando istruzioni KQL
- Renderizzare la visualizzazione usando istruzioni KQL
- Estrarre dati da stringhe non strutturate usando KQL
- Estrarre dati da stringhe strutturate usando KQL
- Creare Funzioni usando KQL

Modulo 5: Configurare il tuo ambiente Azure Sentinel

Inizia con Azure Sentinel configurando in maniera adeguata lo spazio di lavoro Azure Sentinel. I sistemi di informazioni di sicurezza tradizionali e gestione degli eventi (SIEM) solitamente richiedono molto tempo per essere impostati e configurati. Inoltre, non sono necessariamente pensati per carichi di lavoro su cloud. Azure Sentinel ti permette di ottenere rapidamente degli importanti dettagli di sicurezza dai dati locali e sul tuo cloud. Questo modulo ti aiuta a muovere i primi passi in questo contesto. Impara l'architettura degli spazi di lavoro di Azure Sentinel per assicurarti di configurare il tuo sistema affinché soddisfi i requisiti di sicurezza delle operazioni aziendali. In quanto Security Operations Analyst, devi comprendere tabelle, campi e dati compresi nel tuo spazio di lavoro. Scopri come ricercare le tabelle con dati più utilizzate su Azure Sentinel.

Lezioni

- Introduzione a Azure Sentinel
- Creare e gestire spazi di lavoro Azure Sentinel
- Log delle query su Azure Sentinel
- Usare watchlist su Azure Sentinel
- Usare le informazioni sulle minacce su Azure Sentinel

Lab : Configurare il tuo ambiente Azure Sentinel

- Creare uno Spazio di Lavoro Azure Sentinel
- Creare una Watchlist
- Creare un Indicatore di Minaccia

Dopo aver completato questo modulo, gli studenti saranno in grado di:

- Identificare le varie componenti e funzionalità di Azure Sentinel.
- Identificare casi d'uso in cui Azure Sentinel sarebbe una buona soluzione.
- Descrivere l'architettura dello spazio di lavoro Azure Sentinel
- Installare uno spazio di lavoro Azure Sentinel
- Gestire uno spazio di lavoro Azure Sentinel
- Creare una watchlist su Azure Sentinel
- Usare KQL per accedere alla watchlist su Azure Sentinel
- Gestire gli indicatori di minaccia su Azure Sentinel
- Usare KQL per accedere agli indicatori di minaccia su Azure Sentinel

Modulo 6: Connettere i registri a Azure Sentinel

Connetti i dati in cloud scale attraverso tutti gli utenti, dispositivi, applicazioni e infrastrutture, sia in sede che in più clouds con Azure Sentinel. L'approccio principale per connettere i dati dei registri prevede l'uso dei connettori dati forniti da Azure Sentinel. Questo modulo offre una panoramica sui connettori dati disponibili. Imparerai le opzioni di configurazione e i dati forniti dai connettori Azure Sentinel per Microsoft 365 Defender.

Lezioni

- Connettere dati a Azure Sentinel usando connettori dati
- Connettere i servizi Microsoft a Azure Sentinel
- Connettere Microsoft 365 Defender a Azure Sentinel
- Connettere gli host Windows a Azure Sentinel
- Connettere i registri Common Event Format a Azure Sentinel
- Connettere fonti dati syslog a Azure Sentinel
- Connettere indicatori di minaccia a Azure Sentinel

Lab : Connettere registri a Azure Sentinel

- Connettere servizi Microsoft a Azure Sentinel
- Connettere host Windows a Azure Sentinel
- Connettere host Linux a Azure Sentinel
- Connettere informazioni sulle minacce a Azure Sentinel

Dopo aver completato questo modulo, gli studenti saranno in grado di:

- Spiegare l'uso dei connettori dati su Azure Sentinel
- Spiegare le differenze dei connettori Common Event Format e Syslog su Azure Sentinel
- Connettere connettori di servizi Microsoft
- Spiegare come i connettori autocreano incidenti su Azure Sentinel
- Attivare il connettore Microsoft 365 Defender su Azure Sentinel
- Connettere Azure Windows Virtual Machines a Azure Sentinel
- Connettere host Windows non-Azure a Azure Sentinel
- Configurare un agente per l'Analisi dei Registri per raccogliere eventi Sysmon
- Spiegare le opzioni di distribuzione del connettore Common Event Format su Azure Sentinel
- Configurare il connettore TAXII su Azure Sentinel
- Visualizzare gli indicatori di minaccia su Azure Sentinel

Modulo 7: Rilevare ed eseguire analisi usando Azure Sentinel

Scopri delle minacce che non ancora non conoscevi e ponivi rapidamente rimedio con la strumentazione e l'automazione integrate in Azure Sentinel. Imparerai come creare playbook Azure Sentinel per rispondere alle minacce di sicurezza. Esaminerai la gestione degli incidenti di Azure Sentinel, scoprirai gli eventi e le entità di Azure Sentinel e modi per risolvere gli incidenti. Imparerai anche a ricercare, visualizzare e monitorare dati su Azure Sentinel.

Lezioni

- Rilevamento delle minacce con l'analisi di Azure Sentinel
- Risposta alle minacce con playbook di Azure Sentinel
- Gestire gli incidenti di sicurezza su Azure Sentinel
- Usare l'Entity Behavior Analytics su Azure Sentinel

Cercare, visualizzare e monitorare dati su Azure Sentinel

Lab : Rilevare ed eseguire analisi usando Azure Sentinel

- Creare Regole di Analisi
- Modellare degli Attacchi per Definire Attacks to Define una Logica delle Regole
- Mitigare gli Attacchi usando Azure Sentinel
- Creare Cartelle di Lavoro su Azure Sentinel

Dopo aver completato questo modulo, gli studenti saranno in grado di:

- Spiegare l'importanza di Azure Sentinel Analytics.
- Creare regole da template.
- Gestire regole con modifiche.
- Illustrare le potenzialità di Azure Sentinel SOAR.
- Creare un playbook per automatizzare la risposta a un incidente.
- Esaminare e gestire la risoluzione di un incidente.
- Spiegare l'User e l'Entity Behavior Analytics su Azure Sentinel
- Esplorare le entità su Azure Sentinel
- Visualizzare dati di sicurezza usando Azure Sentinel Workbooks.

Modulo 8: Esegui una caccia alle minacce su Azure Sentinel

In questo modulo imparerai ad identificare in maniera proattiva i comportamenti di minaccia usando le query su Azure Sentinel. Imparerai anche a usare i segnalibri e il livestream per dare la caccia alle minacce. Imparerai anche come usare gli appunti su Azure Sentinel per cacce avanzate.

Lezioni

- Scovare le minacce con Azure Sentinel
- Scovare le minacce usando gli appunti su Azure Sentinel

Lab : Dare la caccia alle minacce su Azure Sentinel

- Scovare le Minacce su Azure Sentinel
- Scovare le Minacce usando gli Appunti

Dopo aver completato questo modulo, gli studenti saranno in grado di:

- Illustrare i concetti di caccia alle minacce in rapporto all'uso di Azure Sentinel
- Definire delle ipotesi di caccia alle minacce per l'uso su Azure Sentinel
- Usare query per scovare le minacce.
- Osservare le minacce nel corso del tempo con livestream.
- Esplorare le librerie API per scovare le minacce avanzate su Azure Sentinel
- Creare e usare appunti su Azure Sentinel