MSEC-5 - MOC SC-100T00 - MICROSOFT CYBERSECURITY ARCHITECT

Categoria: **MS Security**

INFORMAZIONI SUL CORSO

Durata:	Categoria:	Qualifica Istruttore:	Dedicato a:	Produttore:
4 Giorni	MS Security	Microsoft Certified Trainer	Professionista IT	Microsoft

OBIETTIVI

-Progettare una strategia e un'architettura Zero Trust
-Valutare strategie tecniche di conformità ai rischi di governance e strategie per le operazioni di sicurezza
-Progettare la sicurezza per l'infrastruttura
-Progettare una strategia per i dati e le applicazioni

PREREQUISITI

Prima di partecipare a questo corso, gli studenti devono dimostrare di avere:
-Esperienza e conoscenza avanzate in materia di identità e accesso, protezione della piattaforma, operazioni di sicurezza, protezione dei dati e protezione delle applicazioni.
-Esperienza con implementazioni cloud e ibride.

CONTENUTI

Modulo 1: Creare una strategia e un'architettura di sicurezza generali
-Introduzione
-Panoramica di Zero Trust
-Sviluppare i punti di integrazione in un'architettura
-Sviluppare i requisiti di sicurezza in base agli obiettivi aziendali
-Tradurre i requisiti di sicurezza in funzionalità tecniche
-Progettare la sicurezza per una strategia di resilienza
-Progettare una strategia di sicurezza per ambienti multi-tenant e ibridi
-Progettare le strategie tecniche e di governance per filtrare e segmentare il traffico
-Informazioni sulla sicurezza per i protocolli
-Esercizio: Creare una strategia e un'architettura di sicurezza generali
-Verifica delle conoscenze
-Riepilogo

Modulo 2: Progettare una strategia per le operazioni di sicurezza
-Introduzione

-Comprendere i framework, i processi e le procedure delle operazioni di sicurezza
-Progettare una strategia di registrazione e di controllo della sicurezza
-Sviluppare operazioni di sicurezza per ambienti multi-cloud e ibridi
-Progettare una strategia SIEM (Security Information and Event Management) e di orchestrazione della sicurezza.
-Valutare i flussi di lavoro di sicurezza
-Esaminare le strategie di sicurezza per la gestione degli eventi imprevisti
-Valutare la strategia delle operazioni di sicurezza per la condivisione dell'intelligence tecnica sulle minacce
-Monitorare le origini delle informazioni dettagliate sulle minacce e le mitigazioni

Modulo 3: Progettare una strategia di sicurezza delle identità

-Introduzione
-Proteggere l'accesso alle risorse cloud
-Consigliare un archivio identità per la sicurezza
-Consigliare strategie sicure di autenticazione e di autorizzazione di sicurezza
-Proteggere l'accesso condizionale
-Progettare una strategia per l'assegnazione e la delega del ruolo
-Definire la governance delle identità per le verifiche di accesso e la gestione degli entitlement
-Progettare una strategia di sicurezza per l'accesso dei ruoli con privilegi all'infrastruttura
-Progettare una strategia di sicurezza per le attività con privilegi
-Informazioni sulla sicurezza per i protocolli

Modulo 4: Valutare una strategia di conformità alle normative

-Introduzione
-Interpretare i requisiti di conformità e le relative funzionalità tecniche
-Valutare la conformità dell'infrastruttura usando Microsoft Defender per il cloud
-Interpretare i punteggi di conformità e consigliare le azioni per risolvere i problemi o migliorare la sicurezza
-Progettare e convalidare l'implementazione di Criteri di Azure
-Progettare i requisiti di residenza dei dati
-Tradurre i requisiti di privacy in requisiti per le soluzioni di sicurezza

Modulo 5: Valutare il comportamento di sicurezza e consigliare strategie tecniche per gestire i rischi

-Introduzione
-Valutare i comportamenti di sicurezza usando i benchmark
-Valutare i comportamenti di sicurezza usando Microsoft Defender per il cloud
-Valutare i comportamenti di sicurezza usando Secure Score
-Valutare la protezione della sicurezza dei carichi di lavoro nel cloud
-Progettare la sicurezza per una zona di destinazione di Azure
-Interpretare l'intelligence tecnica sulle minacce e consigliare le mitigazioni dei rischi
-Consigliare funzionalità o controlli di sicurezza per attenuare i rischi identificati

Modulo 6: Comprendere le procedure consigliate per l'architettura e come cambiano con il cloud

-Introduzione
-Pianificare e implementare una strategia di sicurezza tra i team
-Stabilire una strategia e un processo per l'evoluzione proattiva e continua di una strategia di sicurezza
-Informazioni sui protocolli di rete e sulle procedure consigliate per segmentare la rete e filtrare il traffico

Modulo 7: Progettare una strategia per proteggere gli endpoint server e client

-Introduzione
-Specificare le baseline di sicurezza per gli endpoint server e client

-Specificare i requisiti di sicurezza per i server
-Specificare i requisiti di sicurezza per i dispositivi mobili e i client
-Specificare i requisiti per la protezione di Active Directory Domain Services
-Progettare una strategia per gestire segreti, chiavi e certificati
-Progettare una strategia per l'accesso remoto sicuro
-Comprendere i framework, i processi e le procedure delle operazioni di sicurezza
-Comprendere le procedure forensi approfondite in base al tipo di risorsa

Modulo 8: Progettare una strategia per proteggere i servizi PaaS, IaaS e SaaS

-Introduzione
-Specificare le baseline di sicurezza per i servizi PaaS
-Specificare le baseline di sicurezza per i servizi IaaS
-Specificare le baseline di sicurezza per i servizi SaaS
-Specificare i requisiti di sicurezza per i carichi di lavoro IoT
-Specificare i requisiti di sicurezza per i carichi di lavoro dei dati
-Specificare i requisiti di sicurezza per i carichi di lavoro Web
-Specificare i requisiti di sicurezza per i carichi di lavoro di archiviazione
-Specificare i requisiti di sicurezza per i contenitori
-Specificare i requisiti di sicurezza per l'orchestrazione dei contenitori

Modulo 9: Specificare i requisiti di sicurezza per le applicazioni

-Introduzione
-Comprendere la modellazione delle minacce alle applicazioni
-Specificare le priorità per mitigare le minacce alle applicazioni
-Specificare uno standard di sicurezza per l'onboarding di una nuova applicazione
-Specificare una strategia di sicurezza per le applicazioni e le API

Modulo 10: Progettare una strategia per la protezione dei dati

-Introduzione
-Classificare in ordine di priorità le minacce ai dati
-Progettare una strategia per identificare e proteggere i dati sensibili
-Specificare uno standard di crittografia per i dati in transito e inattivi

INFO

Esame: SC-100 - Microsoft Cybersecurity Architect
Materiale didattico: Materiale didattico ufficiale Microsoft in formato digitale
Costo materiale didattico: 260 € incluso nel prezzo del corso a Calendario
Natura del corso: Operativo (previsti lab su PC)