Curso para la preparación de Certificación SC-200 Microsoft

Duración: 75 horas de formación para la preparación**.**

Modalidad: en remoto a través de aula virtual.

Objetivos del curso:

Una vez finalizado el curso el alumno habrás adquirido los siguientes conocimientos y habilidades para poder investigar y detectar amenazas, así como de responder a ellas, mediante Microsoft Sentinel, Microsoft Defender for Cloud, Microsoft 365 Defender y productos de seguridad de terceros.

Conocimientos previos:

- Conocimientos básicos de Microsoft 365 equivalentes a haber realizado el curso Microsoft 365 Fundamentals.
- Comprensión fundamental de los productos de identidad, cumplimiento y seguridad de Microsoft equivalentes a haber realizado el curso Microsoft Security, Compliance, and Identity Fundamentals.
- Comprensión intermedia de Windows 10
- Familiaridad con los servicios de Azure, específicamente Azure SQL Database y Azure Storage.
- Familiaridad con las máquinas virtuales y las redes virtuales de Azure
- Comprensión básica de los conceptos de secuencias de comandos.

Contenidos:

Módulo 1: amenazas con Microsoft 365 Defender

Módulo 2: amenazas con Microsoft Defender para Endpoint

Módulo 3: amenazas con Microsoft Defender for Cloud

Módulo 4: consultas para Microsoft Sentinel usando Kusto Query Language (KQL)

Módulo 5: Configuración de entorno de Microsoft Sentinel

Módulo 6: Conexión de registros a Microsoft Sentinel

Módulo 7: detecciones e investigaciones usando Microsoft Sentinel

Módulo 8: búsqueda de amenazas en Microsoft Sentinel

Nota: las personas que superen como APTAS esta formación optarán al examen de certificación SC-200 Microsoft Security Operations Analyst.