Curso SC-200 Microsoft Security Operations Analyst

Calle de la Basílica, 19
28020 Madrid
(34) 915 53 61 62
www.cas-training.com

WE ARE CAS

Dirigido a:

Esta curso está diseñado para personas que desempeñen un rol de trabajo de **operaciones de seguridad**. Su objetivo es reducir los riesgos de la organización mediante la corrección rápida de ataques activos en el entorno, el asesoramiento sobre mejoras de los procedimientos de protección contra amenazas y la comunicación de las infracciones de directivas de la organización a las partes interesadas pertinentes. Entre sus responsabilidades están la administración y la supervisión de amenazas y la respuesta a estas mediante diferentes soluciones de seguridad en el entorno. El rol se ocupa principalmente de 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. Dado que el analista de operaciones de seguridad es quien va a hacer uso de los resultados operativos de estas herramientas, también es una parte interesada fundamental en la configuración e implementación de estas tecnologías.

Objetivos:

Prepararte para el examen de certificación SC-200 Microsoft Security Operations Analyst.

Requisitos:

- Tener conocimientos básicos de Microsoft 365.
- Tener conocimientos básicos de los productos de identidad, cumplimiento normativo y seguridad de Microsoft.
- Tener conocimiento intermedio de Microsoft Windows.
- Tener conocimientos sobre los servicios de Azure, en particular Azure SQL Database y Azure Storage.
- Estar familiarizado con las máquinas virtuales de Azure y las redes virtuales.
- Tener conocimientos básicos de los conceptos de scripting.
- Es recomendable haber obtenido, previamente, la certificación SC-900 Microsoft Certified: Security, Compliance, and Identity Fundamentals.

Material del curso:

Documentación oficial para el curso SC-200 Microsoft Security Operations Analyst.

Perfil del docente:

- Formador certificado por Microsoft.
- Más de 5 años de experiencia profesional.
- Más de 4 años de experiencia docente.
- Profesional activo en empresas del sector IT.

Metodología:

- "Learning by doing" se centra en un contexto real y concreto, buscando un aprendizaje en equipo para la resolución de problemas en el sector empresarial.
- Aulas con grupos reducidos para que el profesional adquiera la mejor atención por parte de nuestros instructores profesionales.
- El programa de estudios como partners oficiales es confeccionado por nuestro equipo de formación y revisado por las marcas de referencia en el sector.
- La impartición de las clases podrá ser realizada tanto en modalidad Presencial como Virtual.

Examen y Certificación:

Preparación para el examen de certificación:

SC-200 Microsoft Security Operations Analyst

Contenidos:

- Módulo 1: Introducción a la protección contra amenazas de Microsoft 365
- Módulo 2: Mitigación de incidentes con Microsoft 365 Defender
- Módulo 3: Protección de las identidades con Azure AD Identity Protection
- Módulo 4: Remediate risks with Microsoft Defender for Office 365
- Módulo 5: Protege tu entorno con Microsoft Defender for Identity
- Módulo 6: Proteger las aplicaciones y servicios en la nube con Microsoft Defender for Cloud Apps
- Módulo 7: Respuesta a las alertas de prevención de pérdida de datos mediante Microsoft 365
- Módulo 8: Manage insider risk in Microsoft Purview
- Módulo 9: Investigación de amenazas mediante características de auditoría en Microsoft 365 Defender y Microsoft Purview Estándar
- Módulo 10: Investigación de amenazas mediante auditoría en Microsoft 365 Defender y Microsoft Purview (Premium)
- Módulo 11: Investigación de amenazas con búsqueda de contenido en Microsoft Purview
- Módulo 12: Protect against threats with Microsoft Defender for Endpoint
- Módulo 13: Implementación del entorno de Microsoft Defender para punto de conexión
- Módulo 14: Implementación de mejoras de seguridad de Windows con Microsoft Defender para punto de conexión
- Módulo 15: Realización de investigaciones de dispositivos en Microsoft Defender para punto de conexión
- Módulo 16: Realizar acciones en un dispositivo con Microsoft Defender para punto de conexión
- Módulo 17: Llevar a cabo investigaciones sobre evidencias y entidades con Microsoft Defender para punto de conexión
- Módulo 18: Configuración y administración de la automatización con Microsoft Defender para punto de conexión
- Módulo 19: Configuración de alertas y detecciones en Microsoft Defender para punto de conexión
- Módulo 20: Uso de Administración de vulnerabilidades en Microsoft Defender para punto de conexión
- Módulo 21: Explicación de las protecciones de las cargas de trabajo en la nube en Microsoft Defender para la nube
- Módulo 22: Conexión de recursos de Azure a Microsoft Defender para la nube
- Módulo 23: Conexión de recursos que no son de Azure a Microsoft Defender for Cloud
- Módulo 24: Administración de la posición de seguridad en la nube
- Módulo 25: Explicación de las protecciones de las cargas de trabajo en la nube en Microsoft Defender for Cloud
- Módulo 26: Corrección de alertas de seguridad mediante Microsoft Defender for Cloud
- Módulo 27: Construcción de instrucciones KQL para Microsoft Sentinel
- Módulo 28: Uso de KQL para analizar los resultados de consultas
- Módulo 29: Uso de KQL para crear instrucciones de varias tablas
- Módulo 30: Trabajo con datos en Microsoft Sentinel mediante el lenguaje de consulta Kusto
- Módulo 31: Introducción a Microsoft Sentinel
- Módulo 32: Creación y administración de áreas de trabajo de Microsoft Sentinel
- Módulo 33: Registros de consulta en Microsoft Sentinel
- Módulo 34: Uso de listas de reproducción en Microsoft Sentinel

- Módulo 35: Uso de la inteligencia sobre amenazas en Microsoft Sentinel
- Módulo 36: Conexión de datos a Microsoft Sentinel mediante conectores de datos
- Módulo 37: Conexión de servicios Microsoft a Microsoft Sentinel
- Módulo 38: Conexión de Microsoft 365 Defender a Microsoft Sentinel
- Módulo 39: Conexión de hosts de Windows a Microsoft Sentinel
- Módulo 40: Conexión de registros de formato de evento común a Microsoft Sentinel
- Módulo 41: Conexión de orígenes de datos Syslog a Microsoft Sentinel
- Módulo 42: Conexión de indicadores de amenazas a Microsoft Sentinel
- Módulo 43: Detección de amenazas con análisis de Microsoft Sentinel
- Módulo 44: Automatización en Microsoft Sentinel
- Módulo 45: Administración de incidentes de seguridad en Microsoft Sentinel
- Módulo 46: Identificación de amenazas con Análisis de comportamiento
- Módulo 47: Normalización de datos en Microsoft Sentinel
- Módulo 48: Consulta, visualización y supervisión de datos en Microsoft Sentinel
- Módulo 49: Administración de contenido en Microsoft Sentinel
- Módulo 50: Explicación de los conceptos de búsqueda de amenazas en Microsoft Sentinel
- Módulo 51: Búsqueda de amenazas con Microsoft Sentinel
- Módulo 52: Uso de trabajos de búsqueda en Microsoft Sentinel
- Módulo 53: Búsqueda de amenazas con cuadernos en Microsoft Sentinel

CAS TRAINING

UN ESPACIO PARA CRECER

cas-training.com