TEMARIO

Microsoft Security Operations Analyst

Microsoft

SC-200

SIV & DB CLOUD

EXPERIENCIA Y TECNOLOGIA

CONTÁCTENOS

+57 316 3956090
contactenos@siv.com.co
www.siv.com.co
+57 315 2653920
comercial@siv.com.co
www.dbcloud.co

Microsoft Security Operations Analyst

Examen SC-200

Descripción del curso

Aprenda a investigar y buscar amenazas, y a responder a ellas, mediante Microsoft Sentinel, Microsoft Defender for Cloud y Microsoft 365 Defender. En este curso aprenderá a mitigar ciberamenazas mediante estas tecnologías. En concreto, configurará y usará Microsoft Sentinel, así como el lenguaje de consulta Kusto (KQL), para realizar la detección, el análisis y la generación de informes. El curso se diseñó para personas que desempeñan un rol de trabajo de operaciones de seguridad y ayuda a los alumnos a prepararse para el examen SC-200: Microsoft Security Operations Analyst.

Perfil de Audiencia

El rol Microsoft Security Operations Analyst colabora con las partes interesadas de la organización para proteger los sistemas de tecnología de la información de la organización. 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.

Prerrequisitos

Los estudiantes deben comenzar este curso con las siguientes habilidades:

- Conocimientos básicos de Microsoft 365
- Conocimientos básicos de los productos de identidad, cumplimiento normativo y seguridad de Microsoft.

- Conocimientos intermedios de Windows 10
- Conocimientos sobre los servicios de Azure, en particular Azure SQL Database y Azure Storage
- Familiaridad con las máquinas virtuales de Azure y las redes virtuales
- Conocimientos básicos de los conceptos de scripting.

DESCRIPCION MODULOS DE CAPACITACION

Módulo 1: Mitigación de amenazas con Microsoft 365 Defender

Analice datos sobre amenazas en varios dominios y soluciónelas rápidamente con las opciones de orquestación y automatización en Microsoft 365 Defender. Conozca las amenazas de ciberseguridad y cómo las nuevas herramientas de protección contra amenazas de Microsoft protegen a los usuarios, los dispositivos y los datos de la organización. Use las características avanzadas de detección y corrección de amenazas basadas en identidades para proteger las aplicaciones y las identidades de Azure Active Directory de posibles riesgos.

Lecciones

- Introducción a la protección contra amenazas con Microsoft 365
- Mitigación de incidentes con Microsoft 365 Defender
- Corrección de riesgos con Microsoft Defender para Office 365
- Microsoft Defender for Identity
- Protección de las identidades con Azure AD Identity Protection
- Microsoft Defender for Cloud Apps
- Respuesta a las alertas de prevención de pérdida de datos mediante Microsoft 365
- Administración del riesgo interno en Microsoft 365

Laboratorio: Mitigación de amenazas con Microsoft 365 Defender

- Exploración de Microsoft 365 Defender

Después de completar este módulo, los alumnos podrán:

- Explicar cómo evoluciona el panorama de amenazas.
- Administrar incidentes en Microsoft 365 Defender
- Realice una búsqueda avanzada en Microsoft 365 Defender
- Investigar las alertas de Microsoft 365 Defender

- Describir las características de investigación y corrección de Azure Active Directory Identity Protection.
- Explicar cómo Cloud Discovery ayuda a ver lo que sucede en su organización.

Módulo 2: Mitigación de amenazas con Microsoft Defender para punto de conexión

Implemente la plataforma Microsoft Defender for Endpoint para detectar e investigar amenazas avanzadas, así como responder a ellas. Sepa cómo Microsoft Defender para punto de conexión puede ayudar a su organización a mantenerse segura. Aprenda a implementar el entorno de Microsoft Defender para punto de conexión, incluidas la incorporación de dispositivos y la configuración de seguridad. Obtenga información sobre cómo investigar incidentes y alertas con Microsoft Defender para punto de conexión. Realice una búsqueda avanzada y póngase en contacto con expertos en amenazas. También aprenderá a configurar la automatización en Microsoft Defender para punto de conexión mediante la administración de la configuración del entorno. Por último, conocerá los puntos débiles de su entorno mediante Administración de amenazas y vulnerabilidades en Microsoft Defender para punto de conexión.

Lecciones

- Protección contra amenazas con Microsoft Defender para punto de conexión
- Implementación del entorno de Microsoft Defender para punto de conexión
- Implementación de las mejoras de seguridad de Windows
- Realización de investigaciones de dispositivos
- Realización de acciones en un dispositivo
- Realización de investigaciones de evidencias y entidades
- Configuración y administración de la automatización
- Configuración para alertas y detecciones
- Uso de Administración de amenazas y vulnerabilidades

Laboratorio: Mitigación de amenazas mediante Microsoft 365 Defender para punto de conexión

- Implementación de Microsoft Defender para punto de conexión
- Mitigación de ataques mediante Defender para punto de conexión.

Después de completar este módulo, los alumnos podrán:

- Definir las funcionalidades de Microsoft Defender para punto de conexión.

- Configuración de Microsoft Defender para punto de conexión
- Configurar reglas de reducción de la superficie expuesta a ataques en dispositivos con Windows
- Describir la información de análisis forenses del dispositivo recopilada por Microsoft Defender para punto de conexión
- Realizar la recopilación de datos forenses con Microsoft Defender para punto de conexión
- Investigar cuentas de usuario en Microsoft Defender para punto de conexión
- Administrar la configuración de automatización en Microsoft Defender para punto de conexión
- Administrar los indicadores en Microsoft Defender para punto de conexión
- Describir la capacidad de Administración de amenazas y vulnerabilidades en Microsoft Defender para punto de conexión.

Módulo 3: Mitigación de amenazas con Microsoft Defender for Cloud

Use Microsoft Defender for Cloud, para la seguridad y la protección de cargas de trabajo locales, en Azure y en la nube híbrida. Obtenga información sobre el propósito de Microsoft Defender para la nube y cómo habilitarlo. También conocerá las protecciones y detecciones que proporciona Microsoft Defender for Cloud para cada carga de trabajo en la nube. Obtenga información sobre cómo agregar funcionalidades de Microsoft Defender for Cloud a su entorno híbrido.

Lecciones

- Explicación de las protecciones de las cargas de trabajo en la nube en Microsoft Defender para la nube
- Protección de cargas de trabajo de Microsoft Defender for Cloud
- Conexión de recursos de Azure a Microsoft Defender para la nube
- Conexión de recursos que no son de Azure a Microsoft Defender for Cloud
- Corrección de alertas de seguridad mediante Microsoft Defender for Cloud

Laboratorio: Mitigación de amenazas con Microsoft Defender for Cloud

- Implementación de Microsoft Defender for Cloud
- Mitigación de ataques con Microsoft Defender for Cloud

Después de completar este módulo, los alumnos podrán:

- Descripción de Microsoft Defender para características en la nube
- Explicación de qué cargas de trabajo están protegidas por Microsoft Defender for Cloud
- Explicación del funcionamiento de las protecciones de Microsoft Defender for Cloud

- Configurar el aprovisionamiento automático en Microsoft Defender para la nube
- Describir el aprovisionamiento manual en Microsoft Defender para la nube
- Conexión de máquinas que no son de Azure a Microsoft Defender para la nube
- Descripción de alertas en Microsoft Defender for Cloud
- Corrección de alertas en Microsoft Defender for Cloud
- Automatización de respuestas en Microsoft Defender for Cloud

Módulo 4: Creación de consultas para Microsoft Sentinel mediante el Lenguaje de consulta de Kusto (KQL)

Escriba instrucciones en Lenguaje de consulta de Kusto (KQL) para consultar los datos de registro para realizar detecciones, análisis e informes en Microsoft Sentinel. Este módulo se centrará en los operadores más usados. Las instrucciones en KQL de ejemplo mostrarán consultas de tabla relacionadas con la seguridad. KQL es el lenguaje de consulta que se usa para analizar datos con el fin de crear análisis, libros y realizar búsquedas en Microsoft Sentinel. Obtenga información sobre cómo la estructura de instrucciones KQL básica proporciona la base para crear instrucciones más complejas. Aprender a resumir y visualizar datos con una instrucción KQL proporciona la base para crear detecciones en Microsoft Sentinel. Aprenda a usar el lenguaje de consulta Kusto (KQL) para manipular los datos de cadena ingeridos de los orígenes de registros.

Lecciones

- Construcción de instrucciones KQL para Microsoft Sentinel
- Uso de KQL para analizar los resultados de consultas
- Uso de KQL para crear instrucciones de varias tablas
- Trabajo con datos de cadena mediante instrucciones KQL

Laboratorio: Creación de consultas para Microsoft Sentinel mediante el Lenguaje de consulta Kusto (KQL)

- Creación de consultas para Microsoft Sentinel mediante el Lenguaje de consulta Kusto (KQL)

Después de completar este módulo, los alumnos podrán:

- Construir instrucciones KQL
- Buscar eventos de seguridad en archivos de registro con KQL
- Filtrar búsquedas en función de la hora del evento, la gravedad, el dominio y otros datos relevantes mediante KQL.

- Resumir datos usando instrucciones KQL.
- Representar visualizaciones con instrucciones KQL.
- Extraer datos de campos de cadena no estructurados usando KQL.
- Extraer datos de datos de cadena estructurados usando KQL.
- Crear funciones con KQL.

Módulo 5: Configuración del entorno de Microsoft Sentinel

Para empezar a trabajar con Microsoft Sentinel, configure correctamente el área de trabajo de Microsoft Sentinel. Los sistemas tradicionales de administración de eventos e información de seguridad (SIEM) suelen tardar mucho tiempo en instalarse y configurarse. Tampoco están diseñados de forma específica para cargas de trabajo en la nube. Microsoft Sentinel permite empezar a obtener conclusiones valiosas sobre la seguridad de los datos en la nube y locales en muy poco tiempo. Este módulo lo ayuda a empezar. Obtenga información sobre la arquitectura de las áreas de trabajo de Microsoft Sentinel para asegurarse de que configura el sistema para satisfacer los requisitos de las operaciones de seguridad de su organización. Como analista de operaciones de seguridad, debe comprender las tablas, los campos y los datos ingeridos en el área de trabajo. Descubra cómo consultar las tablas de datos más utilizadas en Microsoft Sentinel.

Lecciones

- Introducción a Microsoft Sentinel
- Creación y administración de áreas de trabajo de Microsoft Sentinel
- Registros de consulta en Microsoft Sentinel
- Uso de listas de reproducción en Microsoft Sentinel
- Uso de la inteligencia sobre amenazas en Microsoft Sentinel

Laboratorio: Configuración del entorno de Microsoft Sentinel

- Configuración del entorno de Microsoft Sentinel

Después de completar este módulo, los alumnos podrán:

- Identificar los distintos componentes y la funcionalidad de Microsoft Sentinel.
- Identificar los casos de uso en los que Microsoft Sentinel sería una buena solución.
- Describir la arquitectura de un área de trabajo de Microsoft Sentinel
- Instalar un área de trabajo de Microsoft Sentinel
- Administrar un área de trabajo de Microsoft Sentinel

- Creación de una lista de reproducción en Microsoft Sentinel
- Uso de KQL para acceder a la lista de reproducción en Microsoft Sentinel
- Administrar indicadores de amenazas en Microsoft Sentinel
- Usar KQL para acceder a los indicadores de amenazas en Microsoft Sentinel

Módulo 6: Conexión de registros a Microsoft Sentinel

Conecte datos a Microsoft Sentinel a la escala de la nube en todos los usuarios, dispositivos y aplicaciones, así como en la totalidad de la infraestructura, tanto en el entorno local como en varias nubes. El enfoque principal para conectar datos de registro es usar los conectores de datos proporcionados de Microsoft Sentinel. En este módulo, se proporciona información general sobre los conectores de datos disponibles. Podrá conocer las opciones de configuración y los datos proporcionados por los conectores de Microsoft Sentinel para Microsoft 365 Defender.

Lecciones

- Conexión de datos a Microsoft Sentinel mediante conectores de datos
- Conexión de servicios Microsoft a Microsoft Sentinel
- Conexión de Microsoft 365 Defender a Microsoft Sentinel
- Conexión de hosts de Windows a Microsoft Sentinel
- Conexión de registros de formato de evento común a Microsoft Sentinel
- Conexión de orígenes de datos Syslog a Microsoft Sentinel
- Conexión de indicadores de amenazas a Microsoft Sentinel

Laboratorio: Conexión de registros a Microsoft Sentinel

- Conexión de datos a Microsoft Sentinel mediante conectores de datos
- Conexión de dispositivos Windows a Microsoft Sentinel mediante conectores de datos
- Conexión de hosts de Linux a Microsoft Sentinel mediante conectores de datos
- Conexión de inteligencia sobre amenazas a Microsoft Sentinel mediante conectores de datos.

Después de completar este módulo, los alumnos podrán:

- Explicar el uso de los conectores de datos en Microsoft Sentinel.
- Explicar las diferencias entre el formato de evento común y el conector Syslog en Microsoft Sentinel.
- Conectar conectores de servicios de Microsoft.

- Explicar el modo en el que los conectores crean incidentes automáticamente en Microsoft Sentinel.
- Activación del conector de Microsoft 365 Defender en Microsoft Sentinel
- Conectar Azure Windows Virtual Machines a Microsoft Sentinel.
- Conectar hosts Windows que no son de Azure a Microsoft Sentinel.
- Configurar el agente de Log Analytics para recopilar eventos de Sysmon.
- Explicar las opciones de implementación del conector de formato de evento común en Microsoft Sentinel.
- Configuración del conector TAXII en Microsoft Sentinel
- Visualización de indicadores de amenazas en Microsoft Sentinel

Módulo 7: Creación de detecciones y realización de investigaciones con Microsoft Sentinel

Detecte amenazas descubiertas anteriormente y soluciónelas rápidamente con opciones de orquestación y automatización en Microsoft Sentinel. Aprenderá a crear cuadernos de estrategias de Microsoft Sentinel para responder a las amenazas de seguridad. Investigará la administración de incidentes de Microsoft Sentinel, obtendrá información sobre los eventos y las entidades de Microsoft Sentinel, y verá maneras de resolver los incidentes. También aprenderá a consultar, visualizar y supervisar datos en Microsoft Sentinel.

Lecciones

- Detección de amenazas con análisis de Microsoft Sentinel
- Administración de incidentes de seguridad en Microsoft Sentinel
- Respuesta a amenazas con cuadernos de estrategias de Microsoft Sentinel
- Análisis de comportamiento de entidades y usuarios en Microsoft Sentinel
- Consulta, visualización y supervisión de datos en Microsoft Sentinel

Laboratorio: Creación de detecciones y realización de investigaciones con Microsoft Sentinel

- Activación de una regla de seguridad de Microsoft
- Creación de un cuaderno de estrategias
- Creación de una consulta programada
- Descripción del modelado de detección
- Realización de ataques
- Creación de detecciones
- Investigación de incidentes
- Creación de libros

Después de completar este módulo, los alumnos podrán:

- Explicar la importancia de Análisis de Microsoft Sentinel.
- Crear reglas a partir de plantillas
- Administrar reglas con modificaciones
- Explicar las funcionalidades de SOAR de Microsoft Sentinel.
- Crear un cuaderno de estrategias para automatizar la respuesta a incidentes.
- Investigar y administrar la resolución de incidentes.
- Explicar el análisis de comportamiento de entidades y usuarios en Microsoft Sentinel
- Explorar entidades en Microsoft Sentinel
- Visualizar datos de seguridad con libros de Microsoft Sentinel

Módulo 8: Búsqueda de amenazas en Microsoft Sentinel

En este módulo obtendrá información sobre cómo identificar de forma proactiva comportamientos de amenaza mediante consultas de Microsoft Sentinel. También va a aprender a usar marcadores y streaming en vivo para la búsqueda de amenazas. También obtendrá información sobre cómo usar cuadernos en Microsoft Sentinel para realizar búsquedas avanzadas.

Lecciones

- Conceptos de búsqueda de amenazas en Microsoft Sentinel
- Búsqueda de amenazas con Microsoft Sentinel
- Búsqueda de amenazas con cuadernos en Microsoft Sentinel

Laboratorio: Búsqueda de amenazas en Microsoft Sentinel

- Realización de la búsqueda de amenazas en Microsoft Sentinel
- Búsqueda de amenazas mediante cuadernos con Microsoft Sentinel

Después de completar este módulo, los alumnos podrán:

- Describir los conceptos de búsqueda de amenazas para usarlos con Microsoft Sentinel.
- Definir una hipótesis de búsqueda de amenazas para usarla en Microsoft Sentinel.
- Usar consultas para buscar amenazas.
- Observar amenazas a lo largo del tiempo con streaming en vivo.
- Explorar las bibliotecas de API para la búsqueda avanzada de amenazas en Microsoft Sentinel
- Crear y usar cuadernos en Microsoft Sentinel

DESCRIPCION CAPACITACION

Duración de la Capacitación

La capacitación tiene una intensidad de 32 horas.

Fechas y Horario Capacitación

La capacitación en horario nocturno de 6:30 P.M. A 9:30 P.M. hora de Colombia 3 veces por semana.

Plataforma Capacitación

Los alumnos se integran a la plataforma Microsoft Teams teniendo acceso siempre a cada clase, así como a los videos de toda la capacitación**.**

Instructor

Se dispone de un Instructor certificado y calificado con muchos años de experiencia en la implementación de soluciones avanzadas y docencia.

Certificados de Asistencia

Cada alumno recibirá el certificado digital de asistencia al finalizar el entrenamiento.