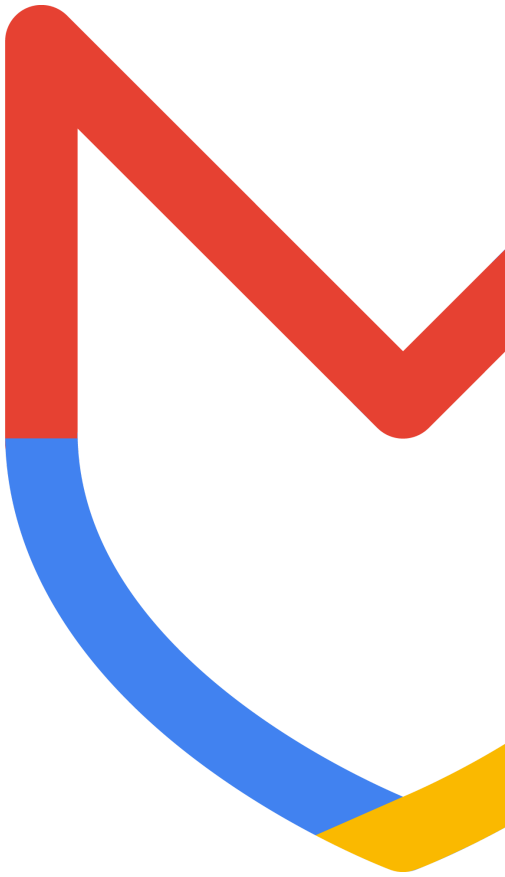
Google Cloud
Security

Academia Mandiant

Respuesta a Incidentes: Guía de Examen



Para obtener más información, visite **https://cloud.google.com/learn/security/mandiant-academy**

Mandiant

Programa de Certificaciones

Mandiant Incident Response (Respuesta a Incidentes de Mandiant)

Examen: MIR-001

Descripción

Este documento tiene como objetivo proporcionar detalles adicionales para el examen de certificación de **Mandiant Incident Response (MIR) .** El examen de certificación MIR verificará que el candidato seleccionado tenga el conocimiento y las habilidades necesarias para investigar, analizar y responder a incidentes de seguridad.

Los exámenes son el resultado de talleres de expertos en la materia y de encuestas de toda la industria sobre las habilidades y conocimientos requeridos de un profesional de **respuesta a incidentes**.

- El examen siguió la norma International *Organization for Standardization* (Organización Internacional de Normalización) conocido como ISO 17024.
- Usando los estándares del *American National Standards Institute* (Instituto Nacional Estadounidense de Estándares) conocido como ANSI para demostrar el cumplimiento.
- Los exámenes se someten a revisiones anuales y actualizaciones de los objetivos según el *National Initiative for Cybersecurity Education* (Iniciativa Nacional para la Educación en Ciberseguridad) conocido como NIST/NICE.
- Utilizando el marco de *Cyber Defense Incident Responder* (Analista de respuesta a incidentes de seguridad) conocido como PR-CIR-001.

Al finalizar el examen, los candidatos recibirán una puntuación de aprobado (70% o más) o no aprobado (69% o menos). Aquellos candidatos con puntaje de aprobación recibirán un certificado y derechos limitados para usar una insignia para firmas electrónicas y credenciales de certificado relacionadas en LinkedIn y/o en su hoja de historial profesional mientras la certificación aún sea válida.

Público objetivo

Este examen recomienda que los candidatos tengan de **tres a cinco años** de experiencia, conocimientos sólidos en habilidades de respuestas de incidentes de seguridad. **Consulte Preparación para el examen** a continuación para obtener más detalles.

Beneficios

- Obtenga certificaciones de clase mundial en dominios de seguridad cibernética
- Mayores oportunidades profesionales
- Mayor seguridad y estabilidad en el empleo
- Mayor credibilidad dentro de la industria de la seguridad cibernética

Método de entrega y duración

La compra de un examen le otorga al candidato el acceso para examinarse una única vez. Mandiant Academy y nuestro socio de pruebas y supervisión, Kryterion, le proporcionarán más detalles. Los exámenes deben completarse dentro de los 90 días posteriores a la compra.

- Supervisión remota en línea (OLP) con la plataforma de pruebas Webassessor de Kryterion
- Registro de autoservicio
- Programación de inscripción abierta dentro de su región local y zona horaria
- Máximo de 50 preguntas
- Preguntas de respuestas múltiples
- Duración de 60 minutos.
- Aprobado (70%)/Solo reprobado: sin puntuación escalada

Renovación de la certificación

Los candidatos deben recertificarse para mantener el estado de su certificación. La certificación es válida por tres años a partir de la fecha de certificación. La recertificación se logra volviendo a completar el examen durante el período de elegibilidad para la recertificación y obteniendo una calificación aprobatoria. Puede intentar la recertificación a partir de 60 días antes de la fecha de vencimiento de su certificación.

Preparación para el examen

Lea este documento detenidamente para revisar los conocimientos generales, las habilidades, las capacidades y las tareas que se evaluarán durante su examen. Tenga en cuenta que los materiales de estudio para este examen no se proporcionarán antes de la fecha programada para el examen. Planifique su cita para el examen en consecuencia si necesita tiempo de estudio para su preparación. Este examen no es en formato de libro abierto y no se permitirán materiales de autoaprendizaje.

Si bien no es obligatorio, el currículum educativo opcional de Mandiant podría ayudar a prepararse para esta certificación basada en habilidades específicas del trabajo. Tenga en cuenta que este examen de

certificación no es una revisión del contenido del material educativo. Estos cursos son únicamente una guía de estudio opcional. Nuestras clases y currículum educativo actuales son solo en inglés.

01	02	03
Fundacional	**Intermedio**	**Avanzado**
Windows Enterprise Incident Response (Respuesta a incidentes empresariales de Windows)	Practical Threat Hunting (Caza de amenazas práctica)	Advanced Windows Incident Response (Respuesta avanzada a incidentes de Windows)
Linux Enterprise Incident Response (Respuesta a incidentes empresariales de Linux)		
Network Traffic Analysis (Análisis de tráfico de red)		

Puede encontrar más información sobre estos cursos en el sitio web de Mandiant Academy . Las listas de conocimientos, habilidades, tareas y capacidades proporcionadas no son exhaustivas. También se pueden incluir en el examen otros ejemplos de tecnologías, procesos o tareas pertenecientes a cada objetivo, aunque no se enumeran ni se tratan en este documento.

Objetivos del examen

El tema cubierto en el examen está asignado a la función de Analista de Respuesta a Incidentes de Seguridad de NIST/NICE e incluye los siguientes temas:

Objetivos:
Conocimiento
Conocimiento de conceptos y protocolos de redes informáticas y metodologías de seguridad de redes.
Conocimiento de los procesos de gestión de riesgos (por ejemplo, métodos para evaluar y mitigar el riesgo).
Conocimiento de las leyes, regulaciones, políticas y ética en relación con la ciberseguridad y la privacidad.
Conocimiento de los principios de ciberseguridad y privacidad.
Conocimiento de ciber amenazas y vulnerabilidades.
Falla el conocimiento de los impactos operativos específicos de la ciberseguridad.
Conocimientos en respaldo y recuperación de datos.
Conocimiento de los planes de continuidad del negocio y recuperación ante desastres de las operaciones.
Conocimiento de los mecanismos de control de acceso al host/red (por ejemplo, lista de control de acceso, lista de capacidades).
Conocimiento de los servicios de red y protocolos de interacción que proporcionan las comunicaciones en red.
Conocimiento de las categorías de incidentes, las respuestas a incidentes y los plazos para las respuestas.
Conocimiento de metodologías de respuesta y manejo de incidentes.
Conocimiento de metodologías y técnicas de detección de intrusiones para detectar intrusiones basadas en host y en red.
Conocimiento de los métodos de análisis del tráfico de red.
Conocimientos en análisis a nivel de paquetes.
Conocimiento de las amenazas y vulnerabilidades de seguridad de sistemas y aplicaciones (p. ej., desbordamiento de búfer, código móvil, secuencias de comandos entre sitios, lenguaje de procedimiento/lenguaje de consulta estructurado [PL/SQL] e inyecciones, condiciones de carrera, canal encubierto, reproducción, ataques orientados al retorno, código malicioso).
Conocimiento de lo que constituye un ataque de red y la relación de un ataque de red con las amenazas y vulnerabilidades.
Conocimiento de políticas, procedimientos y regulaciones de ciberdefensa y seguridad de la información.
Conocimiento de diferentes clases de ataques (por ejemplo, ataques pasivos, activos, internos, cercanos, de distribución).
Conocimiento de los ciberatacantes (por ejemplo, script kiddies, amenazas internas, patrocinados por países no nacionales y patrocinados por naciones).

Conocimiento de técnicas de administración de sistemas, redes y refuerzo de sistemas operativos.
Conocimiento de las etapas del ciberataque (por ejemplo, reconocimiento, escaneo, enumeración, obtención de acceso, escalada de privilegios, mantenimiento del acceso, explotación de la red, cobertura de pistas).
Conocimiento de los conceptos de arquitectura de seguridad de red, incluidos topología, protocolos, componentes y principios (por ejemplo, aplicación de defensa en profundidad).
Conocimiento del modelo OSI y los protocolos de red subyacentes (por ejemplo, TCP/IP).
Conocimiento de los modelos de servicios en la nube y cómo esos modelos pueden limitar la respuesta a incidentes.
Conocimiento de conceptos y metodologías de análisis de malware.
Conocimiento del programa de clasificación de información de una organización y de los procedimientos para comprometer la información.
Conocimiento de protocolos de red como TCP/IP, configuración dinámica de host, sistema de nombres de dominio (DNS) y servicios de directorio.
Conocimiento de los protocolos de enrutamiento y redes comunes (por ejemplo, TCP/IP), los servicios (por ejemplo, web, correo, DNS) y cómo interactúan para proporcionar comunicaciones de red.
Conocimiento de los riesgos de seguridad de las aplicaciones (por ejemplo, lista de los 10 principales proyectos de seguridad de aplicaciones web abiertas).

Habilidades
Habilidad para identificar, capturar, contener y reportar malware.
Habilidad para preservar la integridad de la evidencia de acuerdo con procedimientos operativos estándar o estándares nacionales.
Habilidad para asegurar las comunicaciones en red.
Habilidad para reconocer y categorizar tipos de vulnerabilidades y ataques asociados.
Habilidad en proteger una red contra malware. (por ejemplo, NIPS, antimalware, restringir/prevenir dispositivos externos, filtros de spam).
Habilidad en la realización de evaluaciones de daños.
Habilidad en el uso de herramientas de correlación de eventos de seguridad.
Habilidad para diseñar respuesta a incidentes para modelos de servicios en la nube.

Capacidades
Capacidad para diseñar respuesta a incidentes para modelos de servicios en la nube.
Capacidad para aplicar técnicas para detectar intrusiones basadas en host y en red utilizando tecnologías de detección de intrusiones.

Tareas
Coordine y brinde soporte técnico experto a los técnicos de ciberdefensa de toda la empresa para resolver incidentes de ciberdefensa.
Correlacione los datos de incidentes para identificar vulnerabilidades específicas y hacer recomendaciones que permitan una solución rápida.
Realice análisis de archivos de registro de una variedad de fuentes (por ejemplo, registros de host individuales, registros de tráfico de red, registros de firewall y registros del sistema de detección de intrusiones [IDS (Sistema de detección de intrusiones)]) para identificar posibles amenazas a la seguridad de la red.
Realizar una clasificación de incidentes de defensa cibernética, que incluya determinar el alcance, la urgencia y el impacto potencial, identificar la vulnerabilidad específica y hacer recomendaciones que permitan una solución rápida.
Realizar análisis e informes de tendencias de ciberdefensa.
Realice una recopilación inicial de imágenes con fundamento forense e inspeccione para discernir posibles medidas de mitigación/remediación en los sistemas empresariales.
Realice tareas de manejo de incidentes de ciberdefensa en tiempo real (por ejemplo, recopilaciones forenses, correlación y seguimiento de intrusiones, análisis de amenazas y reparación directa del sistema) para respaldar los equipos de respuesta a incidentes (IRT) desplegables.
Reciba y analice alertas de red de diversas fuentes dentro de la empresa y determine las posibles causas de dichas alertas.
Realice un seguimiento y documente los incidentes de ciberdefensa desde la detección inicial hasta la resolución final.
Redactar y publicar técnicas, orientaciones e informes de defensa cibernética sobre los hallazgos de incidentes para los grupos de interés apropiados.
Emplear principios y prácticas de defensa en profundidad aprobados (por ejemplo, defensa en múltiples lugares, defensas en capas, solidez de la seguridad).
Recopile artefactos de intrusión (por ejemplo, código fuente, malware, troyanos) y utilice los datos descubiertos para permitir la mitigación de posibles incidentes de ciberdefensa dentro de la empresa.
Servir como experto técnico y enlace con el personal encargado de hacer cumplir la ley y explicar los detalles del incidente según sea necesario.
Coordine con analistas de inteligencia para correlacionar los datos de evaluación de amenazas.
Escriba y publique reseñas posteriores a la acción.
Monitorear fuentes de datos externas (por ejemplo, sitios de proveedores de defensa cibernética, equipos de respuesta a emergencias informáticas, enfoque de seguridad) para mantener actualizada la condición de amenaza de defensa cibernética y determinar qué problemas de seguridad pueden tener un impacto en la empresa.
Coordinar las funciones de respuesta a incidentes.

Punto de contacto: mandiant-certification@google.com Programa de certificaciones de Mandiant - Mandiant Academy

Google Cloud

Para obtener más información, visite **https://cloud.google.com/learn/security/mandiant-academy**