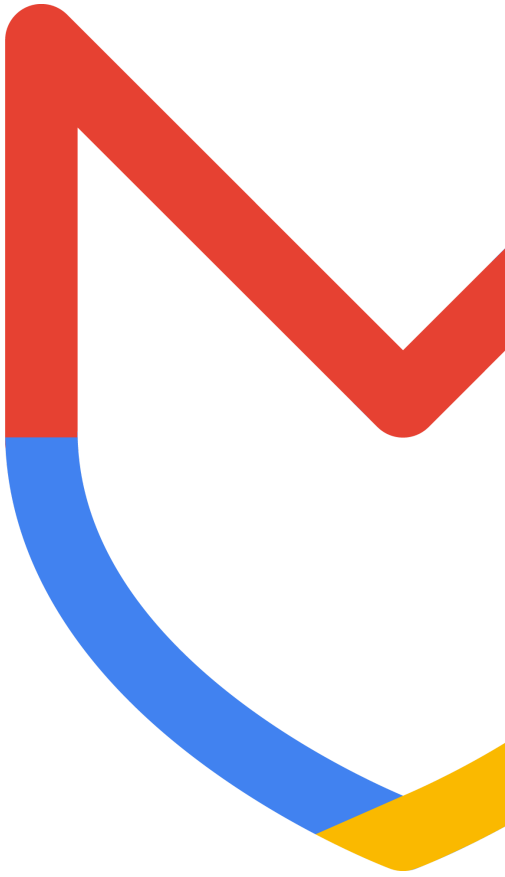
Google Cloud
Security

# Academia Mandiant

Análisis de Inteligencia de Amenazas Cibernéticas: Guía de Examen



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

Mandiant

# Programa de Certificaciones

## Mandiant Cyber Threat Intelligence Analysis (Análisis de inteligencia sobre amenazas cibernéticas de Mandiant)

## Examen: MCTIA-001

**Descripción**

Este documento tiene como objetivo proporcionar detalles adicionales para el examen de certificación **Mandiant Cyber Threat Intelligence Analysis (MCTIA)** . El examen de certificación verificará que el candidato seleccionado tenga la experiencia, el conocimiento y las habilidades progresivas necesarias para investigar, analizar y producir inteligencia para fomentar una postura de seguridad organizacional proactiva.

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 **inteligencia sobre amenazas cibernéticas**.

- 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 *All-Source Analyst* (Analista de todas las fuentes e inteligencia sobre amenazas cibernéticas) conocido como AN-ASA-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 documento 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**

Para este examen se recomienda que los candidatos tengan de **tres a cinco años** de experiencia, conocimientos sólidos y experiencia práctica en inteligencia de amenazas cibernéticas. **Consulte Preparación para el examen** a continuación para obtener más detalles.

**Beneficios**

- Obtenga certificaciones de clase mundial en dominios de seguridad cibernética
- Créditos de CPE para que el personal cumpla con los requisitos de certificación de educación continua
- 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 le evaluarán durante su examen. Tenga en cuenta que los materiales de estudio para este examen en  específico no se proporcionarán antes de la fecha programada para el examen. Planifique su cita para el examen en consecuencia si necesita preparación para el autoestudio. Este examen no es en formato de libro abierto y no se permiten materiales de autoaprendizaje durante el examen supervisado en vivo.

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 exclusivamente en el idioma inglés.

01

**Fundacional**

Cyber Intelligence Foundations (Fundamentos de la ciberinteligencia)

Introductions to Threat Intelligence and Attribution (Introducciones a la inteligencia y atribución de amenazas)

Intelligence Research I-Scoping (I-Alcance de la investigación de inteligencia

02

**Intermedio**

Intelligence Research II-Open Source Intelligences (OSINT) (Investigación de Inteligencia II-Inteligencia de Fuentes Abiertas)

03

**Avanzado**

Cyber Threat Intelligence Production (Producción de inteligencia sobre amenazas cibernéticas)

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 asignado al rol de Analista de todas las fuentes de NIST/NICE e incluye los siguientes temas:

| Objetivos: |
| --- |
| **Conocimiento** |
| Conocimiento de algoritmos de cifrado. |
| Conocimiento de malware. |
| Conocimiento de los ciclos de focalización. |
| Conocimientos de fusión de inteligencia. |

| |
|---|
| Conocimiento de los sesgos cognitivos. |
| Conocimiento de protocolos de redes informáticas. |
| Conocimiento de los procesos de gestión de riesgos. |
| Conocimiento de las leyes y regulaciones de ciberseguridad. |
| Conocimiento de políticas y procedimientos de privacidad. |
| Conocimiento de los principios y prácticas de ciberseguridad. |
| Conocimiento de los principios y prácticas de privacidad. |
| Conocimiento de las amenazas a la ciberseguridad. |
| Conocimiento de las vulnerabilidades de ciberseguridad. |
| Conocimiento de las características de las amenazas a la ciberseguridad. |
| Conocimiento de los principios y prácticas de infraestructura de red. |
| Conocimiento de los principios y prácticas del análisis de requisitos. |
| Conocimiento de las capacidades y aplicaciones de los algoritmos de cifrado. |
| Conocimiento de los principios y prácticas de comunicaciones en red. |
| Conocimiento de los principios y prácticas de interacción persona-computadora (HCI). |
| Conocimiento de las amenazas del sistema. |
| Conocimiento de las vulnerabilidades del sistema. |
| Conocimiento de los principios y prácticas de gestión de activos de datos. |
| Conocimiento de los principios y prácticas de las telecomunicaciones. |
| Conocimiento de los componentes físicos de la computadora. |
| Conocimientos de periféricos de ordenador. |
| Conocimiento de los principios y prácticas de las tácticas adversas. |
| Conocimiento de tácticas, herramientas y técnicas adversas. |
| Conocimiento de tácticas, políticas y procedimientos adversos. |
| Conocimiento de configuraciones de red. |
| Conocimiento de herramientas y técnicas de virtualización de máquinas. |
| Conocimiento de sistemas y software de comunicación digital. |
| Conocimiento de los riesgos de ciberseguridad nuevos y emergentes. |
| Conocimiento de las características de los vectores de amenazas. |
| Conocimiento de los vectores de ataque a la red. |
| Conocimiento de las etapas del ciberataque. |
| Conocimiento de las fases de la actividad de ciber intrusión. |
| Conocimiento de herramientas y técnicas de análisis de malware. |
| Conocimiento de herramientas y técnicas de detección de máquinas virtuales. |
| Conocimiento de estándares de clasificación de datos y mejores prácticas. |
| Conocimiento de herramientas y técnicas de clasificación de datos. |
| Conocimiento del modelo de referencia modelo de interconexión de sistemas abiertos. |
| Conocimiento de las leyes y regulaciones de ciberdefensa. |
| Conocimiento de los principios y prácticas de la arquitectura de red. |
| Conocimiento de los principios y prácticas de análisis de malware. |

| |
|---|
| Conocimiento de herramientas y técnicas de comunicación inalámbrica. |
| Conocimiento de herramientas y técnicas de interferencia de señales. |
| Conocimiento de políticas y procedimientos de clasificación de datos. |
| Conocimiento de las capacidades y aplicaciones del sistema de gestión de contenidos (CMS). |
| Conocimiento de marcos y estándares analíticos. Habilidad para asignar calificaciones de confianza analítica. |
| Conocimiento de herramientas y técnicas de ciberataque. |
| Conocimiento de los principios y prácticas de redes informáticas. |
| Conocimiento de los factores de criticidad en la selección de objetivos. |
| Conocimiento de los factores de vulnerabilidad en la selección de objetivos. |
| Conocimiento de repositorios de información de inteligencia. |
| Conocimiento de los principios y prácticas de operaciones cibernéticas. |
| Conocimiento de herramientas y técnicas de negación y engaño. |
| Conocimiento de sistemas y software de control de supervisión y adquisición de datos (SCADA). |
| Conocimiento de las capacidades y aplicaciones de recopilación de inteligencia. |
| Conocimiento de sistemas y software de tareas de requisitos de inteligencia. |
| Conocimiento de las actividades de apoyo a la inteligencia. |
| Conocimiento de los principios y prácticas de inteligencia de amenazas. |
| Conocimiento de políticas y procedimientos de inteligencia. |
| Conocimiento de los principios y prácticas de abordaje de redes. |
| Conocimiento de los principios y prácticas de seguridad de la red. |
| Conocimiento de herramientas y técnicas de explotación de redes. |
| Conocimiento de las políticas y procedimientos de toma de decisiones. |
| Conocimiento de los principios y prácticas de desarrollo de objetivos. |
| Conocimiento de las herramientas y técnicas de investigación de objetivos. |
| Conocimiento de las políticas y procedimientos de selección de objetivos. |
| Conocimiento de protocolos de enrutamiento. |
| Conocimiento de los procesos de inteligencia. |
| Conocimiento de los procesos de evaluación de operaciones. |
| Conocimiento de conductas de amenaza. |
| Conocimiento de las conductas objetivo. |
| Conocimiento de sistemas y software de amenazas. |
| Conocimiento de máquinas herramienta y tecnologías virtuales. |
| Conocimiento de herramientas y técnicas analíticas. |
| Conocimientos de análisis de datos. |
| Conocimiento de herramientas y técnicas de espacios de trabajo colaborativo virtual. |
| Conocimiento del seguimiento de la fuerza azul. |
| Conocimiento de los requisitos prioritarios de recopilación de inteligencia. |
| Conocimiento de los requisitos prioritarios de inteligencia. |

| Habilidades |
| --- |
| Habilidad para interactuar con los clientes. |
| Habilidad en la realización de investigaciones no atribuibles. |
| Habilidad para comunicar conceptos complejos. |
| Habilidad para colaborar con otros. |
| Habilidad en la creación de análisis de datos. |
| Habilidad para extrapolar a partir de conjuntos de datos incompletos. |
| Habilidad en el análisis de grandes conjuntos de datos. |
| Habilidad en la creación de productos de inteligencia de objetivos. |
| Habilidad para funcionar eficazmente en un entorno dinámico y de ritmo rápido. |
| Habilidad para mitigar sesgos cognitivos. |
| Habilidad para mitigar el engaño en la presentación de informes y análisis. |
| Habilidad para imitar actores de amenazas. |
| Habilidad en el desarrollo de máquinas virtuales. |
| Habilidad en el mantenimiento de máquinas virtuales. |
| Habilidad en la realización de análisis del entorno operativo. |
| Habilidad en la selección de objetivos. |
| Habilidad en la identificación de vulnerabilidades. |
| Habilidad en la realización de análisis de datos de intrusión. |
| Habilidad para identificar las necesidades de información del cliente. |
| Habilidad en evaluación de productos de seguridad. |
| Habilidad para establecer prioridades. |
| Habilidad en la extracción de metadatos. |
| Habilidad en la preparación de entornos operativos. |
| Habilidad para identificar las capacidades de los socios. |
| Habilidad para realizar tácticas de emulación de amenazas. |
| Habilidad para anticipar amenazas. |
| Habilidad para realizar análisis de factores de amenaza. |
| Habilidad en el diseño de sistemas de comunicaciones inalámbricas. |
| Habilidad en la identificación de amenazas en la red. |
| Habilidad en la realización de análisis de capacidades. |
| Habilidad en la realización de análisis de requisitos. |
| Habilidad en la elaboración de reporte. |
| Habilidad para recopilar datos relevantes de una variedad de fuentes. |
| Habilidad para desarrollar requisitos de calificación del puesto. |
| Habilidad para traducir los requisitos operativos en controles de seguridad. |
| Habilidad en la realización de evaluaciones de riesgos. |
| Habilidad para evaluar los efectos generados durante y después de las operaciones cibernéticas. |
| Habilidad para definir un entorno operativo. |
| Habilidad en la realización de análisis de objetivos. |

| |
|---|
| Habilidad en el desarrollo de análisis de datos. |
| Habilidad para evaluar la calidad de las fuentes de datos. |
| Habilidad para evaluar la calidad de la información. |
| Habilidad en la identificación de amenazas de ciberseguridad. |
| Habilidad para identificar brechas de inteligencia. |
| Habilidad en la gestión de relaciones con los clientes. |
| Habilidad en la preparación de reporte de inteligencia. |
| Habilidad en la elaboración de informes posteriores a la acción. |
| Habilidad en consulta de datos. |
| Habilidad para realizar búsquedas de código abierto. |
| Habilidad para incorporar retroalimentación. |
| Habilidad para convertir requerimientos de inteligencia en tareas de producción de inteligencia. |
| Habilidad en el desarrollo de estrategias de recopilación. |
| Habilidad para determinar los requerimientos de información. |
| Habilidad para presentarse ante una audiencia. |
| Habilidad para evaluar las capacidades operativas de los socios. |
| Habilidad para realizar análisis de inteligencia de todas las fuentes. |
| Habilidad para realizar análisis de archivos de registro. |
| Habilidad en la realización de análisis de metadatos. |
| Habilidad en la realización de análisis nodales. |

| Capacidades |
|---|
| Capacidad para atender solicitudes de información. |
| Capacidad para evaluar los procesos de toma de decisiones sobre amenazas. |
| Capacidad para identificar vulnerabilidades de amenazas. |
| Capacidad para facilitar información continuamente actualizada sobre inteligencia, vigilancia y visualización a administradores de imágenes operativas comunes. |
| Capacidad para generar solicitudes de información. |
| Capacidad para identificar brechas y deficiencias de inteligencia. |

| Tareas |
|---|
| Supervise los sitios web de código abierto en busca de contenido hostil dirigido a los intereses de la organización o de los socios. |
| Identificar tácticas y metodologías de amenazas cibernéticas. |
| Determinar los impactos operativos y de seguridad de las fallas de ciberseguridad. |
| Revisar las metas y objetivos de tecnología de la información (TI) empresarial. |
| Estimar el impacto de los daños colaterales. |
| Determine cómo los grupos de actividades de amenazas emplea el cifrado para respaldar sus operaciones. |
| Adquirir identificadores de destino. |

| |
|---|
| Evaluar el desempeño de la operación. |
| Evaluar el impacto de la operación. |
| El análisis de alcance informa a varias audiencias teniendo en cuenta las restricciones de clasificación del intercambio de datos. |
| Determinar si se satisfacen los requisitos de información prioritaria. |
| Identificar actividad anómala de la red. |
| Identificar amenazas potenciales a los recursos de la red. |
| Identificar vulnerabilidades. |
| Recomendar estrategias de remediación de vulnerabilidades. |
| Correlacionar datos de incidentes. |
| Recomendar objetivos de operación cibernética. |
| Determinar la efectividad de las operaciones de recopilación de inteligencia. |
| Recomendar ajustes a las estrategias de recopilación de inteligencia. |
| Asesorar a las partes interesadas sobre el desarrollo del curso de acción. |
| Desarrollar imágenes operativas comunes. |
| Desarrollar indicadores de operaciones cibernéticas. |
| Coordinar las actividades de recolección de todas las fuentes. |
| Validar los requisitos y planes de recopilación de todas las fuentes. |
| Desarrollar requisitos de información prioritaria. |
| Preparar reporte de amenazas y objetivos. |
| Preparar actualizaciones situacionales de amenazas y objetivos. |
| Evaluar los datos de todas las fuentes en busca de valor de inteligencia o vulnerabilidad. |
| Identificar los requisitos de inteligencia. |
| Desarrollar requisitos de recopilación de inteligencia. |
| Designar requisitos de información prioritarios. |
| Modificar requisitos de recopilación. |
| Determinar la efectividad de los requisitos de recopilación. |
| Supervisar los cambios en los conjuntos de problemas de advertencia de operaciones cibernéticas designados. |
| Preparar reporte de cambios para conjuntos de problemas de advertencia de operaciones cibernéticas designados. |
| Monitorear las actividades de amenazas. |
| Preparar reporte de actividad de amenazas. |
| Informar sobre actividades adversas que cumplan requisitos de información prioritaria. |
| Identificar indicaciones y advertencias de cambios de comunicación de destino o fallas de procesamiento. |
| Elaborar reporte de inteligencia de operaciones cibernéticas. |
| Elaborar informes de inteligencia de indicaciones y avisos. |
| Evaluar la eficacia de la producción de inteligencia. |
| Evaluar la eficacia de los informes de inteligencia. |
| Realizar evaluaciones de efectividad posteriores a la acción. |
| Proporcionar análisis de inteligencia y soporte. |

| |
|---|
| Notificar al personal apropiado sobre intenciones o actividades hostiles inminentes. |
| Elaborar informes de intrusión en la red. |
| Determinar si los requisitos de inteligencia y los planes de recopilación son precisos y están actualizados. |

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