Google Cloud
Security

Mandiant Academy

Cyber Threat Intelligence Analysis - Exam Guide

For more information visit **https://cloud.google.com/learn/security/mandiant-academy**

Mandiant

Certifications Program

Mandiant Cyber Threat Intelligence Analysis (MCTIA)
Exam: MCTIA-001

Description

This document is intended to provide additional details for the **Mandiant Cyber Threat Intelligence Analysis (MCTIA)** certification exam. The MCTIA certification exam will verify the successful candidate has the progressive experience, knowledge, and skills required to investigate, analyze, and produce intelligence to foster a proactive organizational security posture.

Exams result from subject matter expert workshops and industry-wide survey results regarding the skills and knowledge required of a cyber threat intelligence professional. Exams undergo annual reviews and updates to the objectives based on the NIST/NICE framework for AN-ASA-001.

Upon completion of the exam, candidates will receive a pass (70%) /fail score. Those candidates with a passing score will be provided with a certification document and limited rights to use a badge for electronic signatures.

Target Audience

This exam is recommended that candidates have **three to five years** of cyber threat intelligence experience and a firm knowledge and hands-on skills relevant to cyber threat intelligence. **See Exam Preparation** below for more details.

Benefits

- Earn World-class certifications in cyber security domains
- Higher career opportunity.
- Increased job security and stability.
- Enhanced credibility within the cyber security industry.

Delivery Method & Duration

Purchasing an exam grants a candidate access to complete one exam attempt. Mandiant Academy and our testing and proctoring partner, Kryterion will provide details. Exams should be completed within 90 days of purchase.

- Remote, online proctored (OLP) with Kryterion's Webassessor testing platform.
- Self-service registration.
- Open Enrollment scheduling within your local region and time zone.
- Maximum of 50 questions.
- Multiple-choice questions.
- 60-minutes duration.
- Pass (70%) / Fail only - no scaled score.

Exam Preparation

Please read this document thoroughly to review the general knowledge, skills, abilities, and tasks you would be evaluated on during your examination. Please be aware study materials for this specific exam will not be provided before your scheduled exam date. Plan your exam appointment accordingly if self-study preparation is needed. This exam is not an open-book format and self-study materials are not allowed during the live, proctored exam.

While not required, optional Mandiant courseware could assist to prepare for this job specific skill-based certification. Please be advised, this certification exam is not a content exam review of the courseware. These courses are an optional study guide only.

01	02	03
Foundational	**Intermediate**	**Advanced**
Cyber Intelligence Foundations	Intelligence Research II-Open Source Intelligence (OSINT)	Cyber Threat Intelligence Production
Introductions to Threat Intelligence and Attribution		
Intelligence Research I-Scoping		

More information about these courses can be found on the Mandiant Academy website. The lists of knowledge, skills, tasks, and abilities provided are not exhaustive. Other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam although not listed or covered in this document.

Exam Objectives

Subject matter covered on the exam mapped to NIST/NICE All Source Analyst role and includes the topics below:

Objectives:
Knowledge
Knowledge of encryption algorithms.
Knowledge of malware.
Knowledge of targeting cycles.
Knowledge of intelligence fusion.
Knowledge of cognitive biasesc.
Knowledge of computer networking protocols.
Knowledge of risk management processes.
Knowledge of cybersecurity laws and regulations.
Knowledge of privacy policies and procedures.
Knowledge of cybersecurity principles and practices.
Knowledge of privacy principles and practices.
Knowledge of cybersecurity threats.
Knowledge of cybersecurity vulnerabilities.
Knowledge of cybersecurity threat characteristics.
Knowledge of network infrastructure principles and practices.
Knowledge of requirements analysis principles and practices.
Knowledge of encryption algorithm capabilities and applications.
Knowledge of network communications principles and practices.
Knowledge of human-computer interaction (HCI) principles and practices.
Knowledge of system threats.
Knowledge of system vulnerabilities.
Knowledge of data asset management principles and practices.
Knowledge of telecommunications principles and practices.
Knowledge of physical computer components.
Knowledge of computer peripherals.
Knowledge of adversarial tactics principles and practices.
Knowledge of adversarial tactics, tools, and techniques.
Knowledge of adversarial tactics, policies, and procedures.
Knowledge of network configurations.
Knowledge of machine virtualization tools and techniques.
Knowledge of digital communication systems and software.

Knowledge of new and emerging cybersecurity risks.
Knowledge of threat vector characteristics.
Knowledge of network attack vectors.
Knowledge of cyber attack stages.
Knowledge of cyber intrusion activity phases.
Knowledge of malware analysis tools and techniques.
Knowledge of virtual machine detection tools and techniques.
Knowledge of data classification standards and best practices.
Knowledge of data classification tools and techniques.
Knowledge of the Open Systems Interconnect (OSI) reference model.
Knowledge of cyber defense laws and regulations.
Knowledge of network architecture principles and practices.
Knowledge of malware analysis principles and practices.
Knowledge of wireless communication tools and techniques.
Knowledge of signal jamming tools and techniques.
Knowledge of data classification policies and procedures.
Knowledge of content management system (CMS) capabilities and applications.
Knowledge of analytic standards and frameworks Skill in assigning analytical confidence ratings.
Knowledge of cyber-attack tools and techniques.
Knowledge of computer networking principles and practices.
Knowledge of target selection criticality factors.
Knowledge of target selection vulnerability factors.
Knowledge of intelligence information repositories.
Knowledge of cyber operations principles and practices.
Knowledge of denial and deception tools and techniques.
Knowledge of supervisory control and data acquisition (SCADA) systems and software
Knowledge of intelligence collection capabilities and applications.
Knowledge of intelligence requirements tasking systems and software.
Knowledge of intelligence support activities.
Knowledge of threat intelligence principles and practices.
Knowledge of intelligence policies and procedures.
Knowledge of network addressing principles and practices.
Knowledge of network security principles and practices.
Knowledge of network exploitation tools and techniques.
Knowledge of decision-making policies and procedures.
Knowledge of target development principles and practices.
Knowledge of target research tools and techniques.
Knowledge of target selection policies and procedures.
Knowledge of routing protocols.
Knowledge of intelligence processes.

Knowledge of operation assessment processes.
Knowledge of threat behaviors.
Knowledge of target behaviors.
Knowledge of threat systems and software.
Knowledge of virtual machine tools and technologies.
Knowledge of analytical tools and techniques.
Knowledge of analytics.
Knowledge of virtual collaborative workspace tools and techniques.
Knowledge of blue force tracking.
Knowledge of priority intelligence collection requirements.
Knowledge of priority intelligence requirements.

Skills
Skill in interfacing with customers.
Skill in conducting non-attributable research.
Skill in communicating complex concepts.
Skill in collaborating with others.
Skill in creating analytics.
Skill in extrapolating from incomplete data sets.
Skill in analyzing large data sets.
Skill in creating target intelligence products.
Skill in functioning effectively in a dynamic, fast-paced environment.
Skill in mitigating cognitive biases.
Skill in mitigating deception in reporting and analysis.
Skill in mimicking threat actors.
Skill in developing virtual machines.
Skill in maintaining virtual machines.
Skill in performing operational environment analysis.
Skill in selecting targets.
Skill in identifying vulnerabilities.
Skill in performing intrusion data analysis.
Skill in identifying customer information needs.
Skill in evaluating security products.
Skill in establishing priorities.
Skill in extracting metadata.
Skill in preparing operational environments.
Skill in identifying partner capabilities.
Skill in performing threat emulation tactics.
Skill in anticipating threats.
Skill in performing threat factor analysis.

Skill in designing wireless communications systems.
Skill in identifying network threats.
Skill in performing capabilities analysis.
Skill in performing requirements analysis.
Skill in preparing reports.
Skill in collecting relevant data from a variety of sources.
Skill in developing position qualification requirements.
Skill in translating operational requirements into security controls.
Skill in performing risk assessments.
Skill in assessing effects generated during and after cyber operations.
Skill in defining an operational environment.
Skill in performing target analysis.
Skill in developing analytics.
Skill in evaluating data source quality.
Skill in evaluating information quality.
Skill in identifying cybersecurity threats.
Skill in identifying intelligence gaps.
Skill in managing client relationships.
Skill in preparing briefing.
Skill in producing after-action reports.
Skill in querying data.
Skill in conducting open-source searches.
Skill in incorporating feedback.
Skill in converting intelligence requirements into intelligence production tasks.
Skill in developing collection strategies.
Skill in determining information requirements.
Skill in presenting to an audience.
Skill in assessing partner operations capabilities.
Skill in performing all-source intelligence analysis.
Skill in performing log file analysis.
Skill in performing metadata analysis.
Skill in performing nodal analysis.

Abilities
Ability to answer requests for information.
Ability to evaluate threat decision-making processes.
Ability to identify threat vulnerabilities.
Ability to facilitate continuously updated intelligence, surveillance, and visualization input to common operational picture managers.
Ability to generate requests for information.

For more information visit **https://cloud.google.com/learn/security/mandiant-academy**

Ability to identify intelligence gaps and shortfalls.

Tasks
Monitor open source websites for hostile content directed towards organizational or partner interests.
Identify cyber threat tactics and methodologies.
Determine the operational and safety impacts of cybersecurity lapses.
Review enterprise information technology (IT) goals and objectives.
Estimate the impact of collateral damage.
Determine how threat activity groups employ encryption to support their operations.
Acquire target identifiers.
Assess operation performance.
Assess operation impact.
Scope analysis reports to various audiences that accounts for data sharing classification restrictions.
Determine if priority information requirements are satisfied.
Identify anomalous network activity.
Identify potential threats to network resources.
Identify vulnerabilities.
Recommend vulnerability remediation strategies.
Correlate incident data.
Recommend cyber operation targets.
Determine effectiveness of intelligence collection operations.
Recommend adjustments to intelligence collection strategies.
Advise stakeholders on course of action development.
Develop common operational pictures.
Develop cyber operations indicators.
Coordinate all-source collection activities.
Validate all-source collection requirements and plans.
Develop priority information requirements.
Prepare threat and target briefings.
Prepare threat and target situational updates.
Assess all-source data for intelligence or vulnerability value.
Identify intelligence requirements.
Develop intelligence collection requirements.
Designate priority information requirements.
Modify collection requirements.
Determine effectiveness of collection requirements.
Monitor changes to designated cyber operations warning problem sets.
Prepare change reports for designated cyber operations warning problem sets.
Monitor threat activities.
Prepare threat activity reports.

Report on adversarial activities that fulfill priority information requirements.
Identify indications and warnings of target communication changes or processing failures Prepare cyber operations intelligence reports.
Prepare indications and warnings intelligence reports.
Assess effectiveness of intelligence production.
Assess effectiveness of intelligence reporting.
Conduct post-action effectiveness assessments.
Provide intelligence analysis and support.
Notify appropriate personnel of imminent hostile intentions or activities.
Prepare network intrusion reports.
Determine if intelligence requirements and collection plans are accurate and up-to-date.

Point of Contact: mandiant-certification@google.com Mandiant Certifications Program - Mandiant Academy