Google Cloud
Security

Mandiant Academy

Incident Response - Exam Guide

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

Mandiant

Certifications Program

Mandiant Incident Response (MIR)
Exam: MIR-001

Description

This document is intended to provide additional details for the **Mandiant Incident Response (MIR)** certification exam. The MIR certification exam will verify the successful candidate has the knowledge and skills required to investigate, analyze, and respond to cyber incidents within the network environment or enclave.

Exams result from subject matter expert workshops and industry-wide survey results regarding the skills and knowledge required of an incident response professional. The exam followed the ANSI (American National Standards Institute) ISO 17024 standard to show compliance. Additionally, exams undergo annual reviews and updates to the objectives based on the NIST/NICE framework for PR-CIR-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, limited rights to use a badge for electronic signatures, and limited rights to use related certificate badging on LinkedIn/Resume while the certification is still valid.

Target Audience

This exam is recommended that candidates have **three to five years** of incident response security experience and a firm knowledge and hands-on skills relevant to incident response **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 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

Certification Renewal/Recertification

Candidates must recertify in order to maintain their certification status. The **Mandiant Incident Response** certification is valid for three years from the date of certification. Recertification is accomplished by retaking the exam during the recertification eligibility time period and achieving a passing score. You may attempt recertification starting 60 days prior to your certification expiration date.

Target Audience

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

Foundational

Windows Enterprise Incident Response

Linux Enterprise Incident Response

Network Traffic Analysis

02

Intermediate

Practical Threat Hunting

03

Advanced

Advanced Windows Enterprise Incident Response

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 Cyber Defense Incident Responder role and includes the topics below:

Objectives:
Knowledge
Knowledge of computer networking concepts and protocols, and network security methodologies.
Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
Knowledge of cybersecurity and privacy principles.
Knowledge of cyber threats and vulnerabilities.
Knowledge of specific operational impacts of cybersecurity lapses.
Knowledge of data backup and recovery.
Knowledge of business continuity and disaster recovery continuity of operations plans.
Knowledge of host/network access control mechanisms (e.g., access control list, capabilities list).
Knowledge of network services and protocols interactions that provide network communications.
Knowledge of incident categories, incident responses, and timelines for responses.
Knowledge of incident response and handling methodologies.
Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.
Knowledge of network traffic analysis methods.
Knowledge of packet-level analysis.
Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).
Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.
Knowledge of cyber defense and information security policies, procedures, and regulations.
Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).
Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored).
Knowledge of system administration, network, and operating system hardening techniques.

Knowledge of cyber-attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).
Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).
Knowledge of cloud service models and how those models can limit incident response.
Knowledge of malware analysis concepts and methodologies.
Knowledge of an organization's information classification program and procedures for information compromise.
Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.
Knowledge of the common networking and routing protocols (e.g., TCP/IP), services (e.g., web, mail, DNS), and how they interact to provide network communications.
Knowledge of Application Security Risks (e.g., Open Web Application Security Project Top 10 list).

Skills
Skill of identifying, capturing, containing, and reporting malware.
Skill in preserving evidence integrity according to standard operating procedures or national standards.
Skill in securing network communications.
Skill in recognizing and categorizing types of vulnerabilities and associated attacks.
Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).
Skill in performing damage assessments.
Skill in using security event correlation tools.
Skill to design incident response for cloud service models.

Abilities
Ability to design incident response for cloud service models.
Ability to apply techniques for detecting host and network-based intrusions using intrusion detection technologies.

Tasks
Coordinate and provide expert technical support to enterprise-wide cyber defense technicians to resolve cyber defense incidents.
Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation.

Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system [IDS (Intrusion Detection System)] logs) to identify possible threats to network security.
Perform cyber defense incident triage, to include determining scope, urgency, and potential impact, identifying the specific vulnerability, and making recommendations that enable expeditious remediation.
Perform cyber defense trend analysis and reporting.
Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems.
Perform real-time cyber defense incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs).
Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.
Track and document cyber defense incidents from initial detection through final resolution.
Write and publish cyber defense techniques, guidance, and reports on incident findings to appropriate constituencies.
Employ approved defense-in-depth principles and practices (e.g., defense-in-multiple places, layered defenses, security robustness).
Collect intrusion artifacts (e.g., source code, malware, Trojans) and use discovered data to enable mitigation of potential cyber defense incidents within the enterprise.
Serve as technical expert and liaison to law enforcement personnel and explain incident details as required.
Coordinate with intelligence analysts to correlate threat assessment data.
Write and publish after action reviews.
Monitor external data sources (e.g., cyber defense vendor sites, Computer Emergency Response Teams, Security Focus) to maintain currency of cyber defense threat condition and determine which security issues may have an impact on the enterprise.
Coordinate incident response functions.

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

Google Cloud

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