EDUSUM

#1 Online Certification Guide

GIAC GEIR

GIAC Enterprise Incident Response Certification Questions & Answers

Exam Summary – Syllabus –Questions

GEIR

GIAC Enterprise Incident Response

82 Questions Exam – 72% Cut Score – Duration of 180 minutes

Table of Contents:

Know Your GEIR Certification Well:

The GEIR is best suitable for candidates who want to gain knowledge in the GIAC Digital Forensics, Incident Response & Threat Hunting. Before you start your GEIR preparation you may struggle to get all the crucial GIAC Enterprise Incident Response materials like GEIR syllabus, sample questions, study guide.

But don't worry the GEIR PDF is here to help you prepare in a stress free manner. The PDF is a combination of all your queries like-

- What is in the GEIR syllabus?
- How many questions are there in the GEIR exam?
- Which Practice test would help me to pass the GEIR exam at the first attempt?

Passing the GEIR exam makes you GIAC Enterprise Incident Response. Having the GIAC Enterprise Incident Response certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

GEIR GIAC Enterprise Incident Response Certification Details:

Exam Name	GIAC Enterprise Incident Response (GEIR)
Exam Code	GEIR
Exam Price	$979 (USD)
Duration	180 mins
Number of Questions	82
Passing Score	72%
Books / Training	**FOR608: Enterprise-Class Incident Response & Threat Hunting**
Schedule Exam	**Pearson VUE**
Sample Questions	**GIAC GEIR Sample Questions**
Practice Exam	**GIAC GEIR Certification Practice Exam**

GEIR Syllabus:

Topic	Details
Cloud Response and Analysis	- The candidate will demonstrate a familiarity with popular cloud attack scenarios and display an understanding of common manual and automated techniques for identifying, extracting, and analyzing artifacts when responding to a cloud-based incident.
Container DFIR Fundamentals	- The candidate will demonstrate a basic understanding of container technology, a familiarity with common attack techniques performed against containers, and a foundational digital forensic and incident response strategy when responding to a container-based incident.
Detecting Modern Attacks	- The candidate will demonstrate an understanding of how to apply threat intelligence and information gathered through proactive threat hunting to support the detection and response to modern attacks.
Enterprise Incident Response Management	- The candidate will demonstrate an understanding of how to manage and conduct effective incident response within an enterprise environment and will display a familiarity with techniques used to address common operational challenges while performing large scale investigations.
Enterprise Visibility and Incident Scoping	- The candidate will demonstrate a familiarity with common data source types in an enterprise environment and will display an understanding of strategies to aggregate telemetry from a large volume of disparate resources in order to scope an incident.
Foundational Cloud Concepts	- The candidate will demonstrate an understanding of fundamental cloud concepts and a familiarity with the most common cloud services that enterprises use to support business operations.
Linux DFIR Fundamentals	- The candidate will demonstrate an understanding of digital forensics and incident response fundamentals for a Linux system, including foundational knowledge of the file system, locations and format of important logs, and key configuration files.
Linux Essentials	- The candidate will demonstrate a basic understanding of a Linux operating system, common challenges when securing and monitoring Linux systems, and popular platform-specific attack techniques across an attack lifecycle.

Topic	Details
macOS DFIR Fundamentals	- The candidate will demonstrate an understanding of digital forensics and incident response fundamentals for a macOS system, including foundational knowledge of the file system, locations and format of important logs, and key configuration files.
macOS Essentials	- The candidate will demonstrate a basic understanding of a macOS operating system, common challenges when securing and monitoring macOS systems, and popular platform-specific attack techniques across an attack lifecycle.
Rapid Response Triage at Scale	- The candidate will demonstrate an understanding of how to efficiently collect, process, and analyze incident response triage data across a large volume of endpoints.

GIAC GEIR Sample Questions:

Question: 1

In the context of rapid response triage at scale, which macOS features assist in remote incident handling?
(Choose Three)

a) Remote Desktop
b) Time Machine
c) Terminal
d) System Preferences
e) Screen Sharing

Answer: a, c, e

Question: 2

Which of the following are essential tools for malware analysis on macOS?
(Choose Two)

a) Terminal
b) Keychain Access
c) Activity Monitor
d) Finder

Answer: a, c

Question: 3

What capabilities should a tool have to effectively collect and process incident response data at scale across macOS endpoints?
(Choose Three)

a) Remote script execution
b) Automatic user logout
c) Network traffic monitoring
d) Live memory analysis
e) System log aggregation

Answer: a, d, e

Question: 4

What is the FIRST step an incident responder should take after identifying an anomaly that could indicate a modern attack?

a) Notify all company employees about the anomaly
b) Isolate the affected system from the network
c) Collect and preserve digital evidence
d) Perform a full system backup

Answer: c

Question: 5

The default location for system log files in a Linux system is _______.

a) /var/log
b) /etc/log
c) /usr/log
d) /home/log

Answer: a

Question: 6

What are effective practices for maintaining enterprise visibility to support incident scoping?

a) Regular data purging to free up storage space
b) Continuous monitoring of network traffic
c) Integrating SIEM solutions for real-time analysis
d) Periodic manual audits of security settings

Answer: b, c

Question: 7

Which tool is primarily used for detailed investigation of the filesystem in Linux DFIR tasks?

a) Grep
b) Sed
c) Awk
d) Debugfs

Answer: d

Question: 8

In a cloud-based incident response, which tool is commonly used to analyze network traffic to and from a cloud environment?

a) Wireshark
b) Splunk
c) Microsoft Excel
d) Adobe Acrobat

Answer: a

Question: 9

Select the macOS features that assist in recovery and backup.
(Multiple Correct Answers)

a) Time Machine
b) Disk Utility
c) Finder
d) Boot Camp
e) Spotlight

Answer: a, b

Question: 10

For analyzing log data effectively, which command is best suited for sorting and extracting specific information?

a) cat
b) grep
c) touch
d) chmod

Answer: b

Study Guide to Crack GIAC Enterprise Incident Response GEIR Exam:

- Getting details of the GEIR syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the GEIR exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the GIAC provided training for GEIR exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the GEIR sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on GEIR practice tests is must. Continuous practice will make you an expert in all syllabus areas.