EDUSUM

#1 Online Certification Guide

GIAC GCTI

GIAC Cyber Threat Intelligence Certification Questions & Answers

Exam Summary – Syllabus –Questions

GCTI

GIAC Cyber Threat Intelligence

82 Questions Exam – 71% Cut Score – Duration of 180 minutes

Table of Contents:

Know Your GCTI Certification Well:

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

But don't worry the GCTI 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 GCTI syllabus?
- How many questions are there in the GCTI exam?
- Which Practice test would help me to pass the GCTI exam at the first attempt?

Passing the GCTI exam makes you GIAC Cyber Threat Intelligence. Having the GIAC Cyber Threat Intelligence certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

GCTI GIAC Cyber Threat Intelligence Certification Details:

Exam Name	GIAC Cyber Threat Intelligence (GCTI)
Exam Code	GCTI
Exam Price	$979 (USD)
Duration	180 mins
Number of Questions	82
Passing Score	71%
Books / Training	**FOR578: Cyber Threat Intelligence**
Schedule Exam	**GIAC**
Sample Questions	**GIAC GCTI Sample Questions**
Practice Exam	**GIAC GCTI Certification Practice Exam**

GCTI Syllabus:

Topic	Details
Analysis of Intelligence	- The candidate will demonstrate an understanding of the techniques employed in analyzing information. The candidate will also demonstrate an understanding obstacles to accurate analysis, such as fallacies and bias, and how to recognize and avoid them.
Campaigns and Attribution	- The candidate will demonstrate an understanding of identifying and profiling intrusion characteristics and external intelligence into campaigns. The candidate will demonstrate an understanding of the importance of attribution and the factors that are considered when making an attribution.
Collecting and Storing Data Sets	- The candidate will demonstrate an understanding of collecting and storing data from collection sources such as threat feeds, domains, TLS certificates, and internal sources.
Intelligence Application	- The candidate will demonstrate an understanding of the practical application of gathering, analyzing, and using intelligence. Additionally, the candidate will demonstrate an understanding of how well-known cyber attacks can inform cyber intelligence professionals today.
Intelligence Fundamentals	- The candidate will demonstrate an understanding of fundamental cyber threat intelligence definitions and concepts. The candidate will also demonstrate a basic working knowledge of technologies that provide intelligence analysts with data, such as network indicators, log repositories, and forensics tools.
Kill Chain, Diamond Model, and Courses of Action Matrix	- The candidate will demonstrate an understanding of the Kill Chain, Diamond Model, and Courses of Actions Matrix and how they are used together to analyze intrusions.
Malware as a Collection Source	- The candidate will demonstrate an understanding of malware analysis tools and techniques to derive intelligence.
Pivoting	- The candidate will demonstrate an understanding of pivoting to expand intelligence, pivot analysis, the ability to use link analysis tools, and ability perform domain analysis to expand intelligence collections.
Sharing Intelligence	- The candidate will demonstrate an understanding of methods and practices of storing intelligence from various sources. The candidate will demonstrate an

Topic	Details
	understanding of the processes, tools, and techniques used in sharing intelligence. The candidate will demonstrate an understanding of effectively sharing tactical intelligence with executives by writing accurate and effective reports and using such capabilities as assessments.

GIAC GCTI Sample Questions:

Question: 1

Which of the following are examples of dynamic analysis tools?
(Select 2)

a) OllyDbg
b) PEiD
c) Cuckoo Sandbox
d) IDA Pro

Answer: a, c

Question: 2

Which data storage strategy is most effective for handling large volumes of threat intelligence data from multiple sources?

a) Relational databases with strict schema
b) Encrypted USB drives for portability
c) Local storage on individual analyst workstations
d) Distributed storage systems with scalable architecture

Answer: d

Question: 3

The Courses of Action Matrix helps analysts determine the best way to _____ a threat.

a) Monitor
b) Ignore
c) Respond to
d) Create

Answer: c

Question: 4

When analyzing intelligence, which cognitive bias involves favoring information that confirms preexisting beliefs or theories?

a) Availability bias
b) Confirmation bias
c) Anchoring bias
d) Hindsight bias

Answer: b

Question: 5

Which of the following is an example of a logical fallacy that could hinder accurate analysis?

a) Hasty generalization
b) Data normalization
c) Algorithm bias
d) Redundancy elimination

Answer: a

Question: 6

During the _____ phase of the Cyber Kill Chain, the adversary exploits a vulnerability to execute code on the victim's system.

a) Reconnaissance
b) Exploitation
c) Delivery
d) Installation

Answer: b

Question: 7

Which of the following best describes the concept of "data normalization" in the context of storing threat intelligence data?

a) Encrypting data to protect it from unauthorized access
b) Reducing the amount of data to save storage space
c) Transforming data into a common format to facilitate analysis and comparison
d) Compressing data to speed up transmission

Answer: c

Question: 8

What are key techniques used in analyzing gathered intelligence?

(Select 3)

a) Vulnerability scanning
b) Intrusion detection
c) Pattern recognition
d) Correlation analysis
e) Trend analysis

Answer: c, d, e

Question: 9

In static malware analysis, which of the following techniques are commonly used?

(Select 3)

a) Code disassembly
b) Behavior monitoring
c) String extraction
d) Network traffic analysis
e) File hashing

Answer: a, c, e

Question: 10

How can intelligence from well-known cyber attacks be used to improve current cybersecurity practices?

(Select 3)

a) Developing new encryption standards
b) Understanding attacker tactics
c) Enhancing incident response plans
d) Designing user-friendly interfaces
e) Training staff on social engineering

Answer: b, c, e

Study Guide to Crack GIAC Cyber Threat Intelligence GCTI Exam:

- Getting details of the GCTI 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 GCTI 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 GCTI 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 GCTI 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 GCTI practice tests is must. Continuous practice will make you an expert in all syllabus areas.