



EC-COUNCIL 312-85 STUDY GUIDE PDF

**Grab the EC-Council Certified Threat Intelligence Analyst
Certification PDF Questions & Answers**

Details of the Exam-Syllabus-Questions

312-85
EC-Council Certified Threat Intelligence Analyst (CTIA)
50 Questions Exam - 70% Cut Score - Duration of 120 minutes

Table of Contents:

Get an Overview of the 312-85 Certification:	2
Why Should You Earn the EC-Council 312-85 Certification?	2
What is the EC-Council 312-85 Certified Threat Intelligence Analyst Certification Exam Structure?	2
Enhance Knowledge with 312-85 Sample Questions:	3
What Study Guide Works Best in acing the EC-Council 312-85 Certified Threat Intelligence Analyst Certification?	6
Explore the Syllabus Topics and Learn from the Core:	6
Make Your Schedule:	6
Get Expert Advice from the Training:	7
Get Access to the PDF Sample Questions:	7
Avoid Dumps and utilize the EC-Council 312-85 Practice Test:	7

Get an Overview of the 312-85 Certification:

Who should take the [312-85 exam](#)? This is the first question that comes to a candidate's mind when preparing for the Certified Threat Intelligence Analyst certification. The 312-85 certification is suitable for candidates who are keen to earn knowledge on the Specialist and grab their EC-Council Certified Threat Intelligence Analyst (CTIA). When it is about starting the preparation, most candidates get confused regarding the study materials and study approach. But 312-85 study guide PDF is here to solve the problem. 312-85 PDF combines some effective sample questions and offers valuable tips to pass the exam with ease.

Why Should You Earn the EC-Council 312-85 Certification?

There are several reasons why one should grab the 312-85 certification.

- The Certified Threat Intelligence Analyst certification proves to be one of the most recognized certifications.
- The certification badge proves the knowledge of the candidate regarding subject matters and makes his resume presentable to potential candidates.
- Thus earning the [EC-Council Certified Threat Intelligence Analyst \(CTIA\)](#) is a powerful qualification for a prosperous career.

What is the EC-Council 312-85 Certified Threat Intelligence Analyst Certification Exam Structure?

Exam Name	EC-Council Certified Threat Intelligence Analyst (CTIA)
Exam Code	312-85
Exam Price	\$250 (USD)
Duration	120 mins
Number of Questions	50
Passing Score	70%
Books / Training	Courseware
Schedule Exam	Pearson VUE OR ECC Exam Center
Sample Questions	EC-Council CTIA Sample Questions
Practice Exam	EC-Council 312-85 Certification Practice Exam

Enhance Knowledge with 312-85 Sample Questions:

Question: 1

Bob, a threat analyst, works in an organization named TechTop. He was asked to collect intelligence to fulfil the needs and requirements of the Red Team present within the organization. Which of the following are the needs of a RedTeam?

- a) Intelligence related to increased attacks targeting a particular software or operating system vulnerability
- b) Intelligence on latest vulnerabilities, threat actors, and their tactics, techniques, and procedures (TTPs)
- c) Intelligence extracted latest attacks analysis on similar organizations, which includes details about latest threats and TTPs
- d) Intelligence that reveals risks related to various strategic business decisions

Answer: b

Question: 2

Which of the following characteristics of APT refers to numerous attempts done by the attacker to gain entry to the target's network?

- a) Risk tolerance
- b) Timeliness
- c) Attack origination points
- d) Multiphased

Answer: c

Question: 3

Jian is a member of the security team at Trinity, Inc. He was conducting a real-time assessment of system activities in order to acquire threat intelligence feeds. He acquired feeds from sources like honeynets, P2P monitoring, infrastructure, and application logs.

Which of the following categories of threat intelligence feed was acquired by Jian?

- a) Internal intelligence feeds
- b) External intelligence feeds
- c) CSV data feeds
- d) Proactive surveillance feeds

Answer: a

Question: 4

In which of the following attacks does the attacker exploit vulnerabilities in a computer application before the software developer can release a patch for them?

- a) Active online attack
- b) Zero-day attack
- c) Distributed network attack
- d) Advanced persistent attack

Answer: b**Question: 5**

Which of the following types of threat attribution deals with the identification of the specific person, society, or a country sponsoring a well-planned and executed intrusion or attack over its target?

- a) Nation-state attribution
- b) True attribution
- c) Campaign attribution
- d) Intrusion-set attribution

Answer: b**Question: 6**

Daniel is a professional hacker whose aim is to attack a system to steal data and money for profit. He performs hacking to obtain confidential data such as social security numbers, personally identifiable information (PII) of an employee, and credit card information.

After obtaining confidential data, he further sells the information on the black market to make money. Daniel comes under which of the following types of threat actor

- a) Industrial spies
- b) State-sponsored hackers
- c) Insider threat
- d) Organized hackers

Answer: d

Question: 7

During the process of threat intelligence analysis, John, a threat analyst, successfully extracted an indication of adversary's information, such as Modus operandi, tools, communication channels, and forensics evasion strategies used by adversaries.

Identify the type of threat intelligence analysis is performed by John.

- a) Operational threat intelligence analysis
- b) Technical threat intelligence analysis
- c) Strategic threat intelligence analysis
- d) Tactical threat intelligence analysis

Answer: d

Question: 8

A network administrator working in an ABC organization collected log files generated by a traffic monitoring system, which may not seem to have useful information, but after performing proper analysis by him. The same information can be used to detect an attack in the network.

Which of the following categories of threat information has he collected?

- a) Advisories
- b) Strategic reports
- c) Detection indicators
- d) Low-level data

Answer: c

Question: 9

In terms conducting data correlation using statistical data analysis, which data correlation technique is a nonparametric analysis, which measures the degree of relationship between two variables?

- a) Pearson's Correlation Coefficient
- b) Spearman's Rank Correlation Coefficient
- c) Kendall's Rank Correlation Coefficient
- d) Einstein-Musk Growth Correlation Coefficient

Answer: b

Question: 10

Cybersol Technologies initiated a cyber-threat intelligence program with a team of threat intelligence analysts. During the process, the analysts started converting the raw data into useful information by applying various techniques, such as machine-based techniques, and statistical methods.

In which of the following phases of the threat intelligence lifecycle is the threat intelligence team currently working?

- a) Dissemination and integration
- b) Planning and direction
- c) Processing and exploitation
- d) Analysis and production

Answer: a

What Study Guide Works Best in acing the EC-Council 312-85 Certified Threat Intelligence Analyst Certification?

The 312-85 study guide is a combination of some proven study tips and the combination of all valuable study materials like sample questions, syllabus and practice tests in one place.

Explore the Syllabus Topics and Learn from the Core:

If you are determined to earn success in the Certified Threat Intelligence Analyst exam, getting in full touch of the [syllabus](#) is mandatory. During preparation, you might not like all syllabus sections or topics, but try to get at least the fundamental knowledge from the sections you don't like. The more you possess knowledge on all syllabus sections, the more is the chance to attempt maximum number of questions during the actual exam.

Make Your Schedule:

Studying and completing the syllabus becomes easier, if you work on the syllabus topics after making a schedule. Your syllabus must mention what areas you want

to cover and within what time. Once you make a schedule and follow it regularly, syllabus completion becomes easier and preparation becomes smoother.

Get Expert Advice from the Training:

Do not forget to join the EC-Council 312-85 training if it is providing any. Training enhances the practical knowledge of a candidate, which helps them to work well in the practical field during projects.

Get Access to the PDF Sample Questions:

If your study material is in a [PDF format](#) or the materials are mobile-friendly, what could be better than that? Get access to the free sample questions and keep enhancing your knowledge beyond the syllabus.

Avoid Dumps and utilize the EC-Council 312-85 Practice Test:

Why should you rely on practice tests? The reason is simple: you must get familiar with the exam pattern before reaching the exam hall. An aspirant aware of the exam structure and time management during the exam preparation can perform well in the actual exam and attempt the maximum number of questions during the exam.

Many aspirants prefer to read from dumps, but they miss out on the self assessment method. Therefore, 312-85 practice tests always stand out to be the better choice than dumps PDF.

Avail the Proven 312-85 Practice Test for Success!!!

Do you want to pass the 312-85 exam on your first attempt? Stop worrying; we, EduSum.com are here to provide you the best experience during your EC-Council Certified Threat Intelligence Analyst preparation. Try out our free mock tests to get a glimpse of our quality study materials, and build your confidence with the premium [312-85 practice tests](#). Our expert-designed questions help you to improve performance and pass the exam on your first attempt.