EC-COUNCIL 312-85

EC-Council CTIA Certification Questions & Answers

Get Instant Access to Vital Exam Acing Materials | Study Guide | Sample Questions | Practice Test

312-85

EC-Council Certified Threat Intelligence Analyst

50 Questions Exam – 70% Cut Score – Duration of 120 minutes




EDUSUM

#1 Online Certification Guide

Table of Contents:

Discover More about the 312-85 Certification

Are you interested in passing the EC-Council 312-85 exam? First discover, who benefits from the 312-85 certification. The 312-85 is suitable for a candidate if he wants to learn about Specialist. Passing the 312-85 exam earns you the EC-Council Certified Threat Intelligence Analyst title.

While preparing for the 312-85 exam, many candidates struggle to get the necessary materials. But do not worry; your struggling days are over. The 312-85 PDF contains some of the most valuable preparation tips and the details and instant access to useful **312-85 study materials just at one click.**

EC-Council 312-85 CTIA Certification Details:

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**

312-85 Syllabus:

Topic
Introduction to Threat Intelligence
Cyber Threats and Kill Chain Methodology
Requirements, Planning, Direction, and Review
Data Collection and Processing
Data Analysis
Intelligence Reporting and Dissemination

Broaden Your Knowledge with EC-Council 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 Tam 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

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: 3

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: 4

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: 5

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: 6

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: 7

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: 8

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

Question: 9

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: 10

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

Avail the Study Guide to Pass EC-Council 312-85 CTIA Exam:

- Find out about the 312-85 syllabus topics. Visiting the official site offers an idea about the exam structure and other important study resources. Going through the syllabus topics help to plan the exam in an organized manner.
- Once you are done exploring the **312-85 syllabus**, it is time to plan for studying and covering the syllabus topics from the core. Chalk out the best plan for yourself to cover each part of the syllabus in a hassle-free manner.
- A study schedule helps you to stay calm throughout your exam preparation. It should contain your materials and thoughts like study hours, number of topics for daily studying mentioned on it. The best bet to clear the exam is to follow your schedule rigorously.
- The candidate should not miss out on the scope to learn from the 312-85 training. Joining the EC-Council provided training for 312-85 exam helps a candidate to strengthen his practical knowledge base from the certification.
- Learning about the probable questions and gaining knowledge regarding the exam structure helps a lot. Go through the **312-85 sample questions** and boost your knowledge
- Make yourself a pro through online practicing the syllabus topics. 312-85 practice tests would guide you on your strengths and weaknesses regarding the syllabus topics. Through rigorous practicing, you can improve the weaker sections too. Learn well about time management during exam and become confident gradually with practice tests.

Career Benefits:

- Passing the 312-85 exam, helps a candidate to prosper highly in his career. Having the certification on the resume adds to the candidate's benefit and helps to get the best opportunities.