EDUSUM

#1 Online Certification Guide

EC-COUNCIL 312-85

EC-Council CTIA Certification Questions & Answers

Exam Summary – Syllabus –Questions

312-85

EC-Council Certified Threat Intelligence Analyst (CTIA)

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

Table of Contents:

Know Your 312-85 Certification Well:

The 312-85 is best suitable for candidates who want to gain knowledge in the EC-Council Specialist. Before you start your 312-85 preparation you may struggle to get all the crucial CTIA materials like 312-85 syllabus, sample questions, study guide.

But don't worry the 312-85 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 312-85 syllabus?
- How many questions are there in the 312-85 exam?
- Which Practice test would help me to pass the 312-85 exam at the first attempt?

Passing the 312-85 exam makes you EC-Council Certified Threat Intelligence Analyst (CTIA). Having the CTIA certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

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

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

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: 3

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: 4

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: 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

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

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 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: 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

Study Guide to Crack EC-Council CTIA 312-85 Exam:

- Getting details of the 312-85 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 312-85 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 EC-Council provided training for 312-85 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 312-85 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 312-85 practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for 312-85 Certification

Make EduSum.com your best friend during your EC-Council Certified Threat Intelligence Analyst exam preparation. We provide authentic practice tests for the 312-85 exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual 312-85 exam. We guarantee you 100% success in your first exam attempt if you continue practicing regularly. Don't bother if you don't get 100% marks in initial practice exam attempts. Just utilize the result section to know your strengths and weaknesses and prepare according to that until you get 100% with our practice tests. Our evaluation makes you confident, and you can score high in the 312-85 exam.

Start Online Practice of 312-85 Exam by visiting URL
https://www.edusum.com/ec-council/312-85-ec-council-certified-threat-intelligence-analyst